UNIVERSIDAD POLITÉCNICA SALESIANA

FACULTAD DE INGENIERÍAS

SEDE QUITO – CAMPUS SUR

CARRERA DE INGENIERÍA DE SISTEMAS

MENCIÓN TELEMÁTICA

“ESTUDIO TÉCNICO – ECONÓMICO PARA LA TRANSICIÓN IPV4 A IPV6 DE UN PUNTO DE INTERCAMBIO DE TRÁFICO DE INTERNET (NAP.EC) QUE UTILIZA BGP COMO PROTOCOLO DE ENRUTAMIENTO”

TESIS PREVIA A LA OBTENCIÓN DE TÍTULO DE INGENIERO DE SISTEMAS

ADRIANA LUCÍA MORALES FLORES

JEANETH VERÓNICA RUCHI YUNGÁN

DIRECTOR: ING. RAFAÉL JAYA

Quito, Diciembre del 2010

DECLARACIÓN

Declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría, y que no ha sido presentado previamente para ningún otro grado o calificación profesional; parte de la información ha sido recabada en la empresa “AEPROVI”: además hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Politécnica Salesiana, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normatividad institucional vigente.

EGR. ADRIANA L. MORALES F.

EGR. JEANETH V. RUCHI Y.

CERTIFICACIÓN

Certifico que el presente trabajo titulado “Estudio técnico – económico para la transición IPv4 a IPv6 de un punto de intercambio de tráfico de Internet (NAP.EC que utiliza BGP como protocolo de enrutamiento” fue desarrollado por las señoritas: Adriana Lucia Morales Flores y Jeaneth Verónica Ruchi Yungán, bajo mi dirección.

_____

Ing. Rafael Jaya

DIRECTOR DE TESIS

AGRADECIMIENTO

Detrás de cada línea de llegada, hay una de partida.
Detrás de cada logro, hay otro desafío.
Si extrañas lo que hacías, vuelve a hacerlo.
Sigue aunque todos esperen que abandones,
No dejes que se oxide el hierro que hay en ti.

Agradecemos principalmente a la Empresa AEPROVI, por todo el apoyo brindado durante el desarrollo de este trabajo.

Al Ingeniero Fabián Mejía, Administrador del NAP.EC, con su profesionalismo y experiencia ha sabido brindarnos conocimientos acertados los mismos que reposan en este trabajo y también por la confianza depositada.

Al Ingeniero Rafael Jaya, Director de Tesis, quien confió en nosotras al darnos su apoyo a lo largo de esta tutoría, por sus guías para la culminación de este proyecto de manera satisfactoria.

A las Autoridades y Docentes de la Facultad, por sus conocimientos impartidos, paciencia, enseñanza y finalmente un eterno agradecimiento a esta prestigiosa Universidad la cual abre sus puertas a jóvenes como nosotros, preparándonos para un futuro competitivo y formándonos como personas de bien.

Adriana Lucía Morales Flores
Jeaneth Verónica Ruchi Yungán

DEDICATORIA

Antes que nada a mi Padre Celestial, quien esta a mi lado en todo momento dándome la fe y fortaleza necesaria para luchar día tras día para salir adelante, rompiendo las barreras que se me presenten y así poder culminar con este gran esfuerzo.

A mis queridos padres Jorge Orlando Morales Morales y María Dolores Flores Suntaxi; por darme la vida, por estar junto a mí en todo momento siendo el pilar fundamental para mi crianza. Es a ellos a quien les debo todo lo que soy, supieron inculcarme valores para formarme como un ser integral del cual me siento orgullosa y finalmente son quienes me han dejado este gran legado que durará por siempre conmigo.

A mis hermanos Liliana y Jorgito por la confianza depositada en mí, su apoyo incondicional en todo momento; fortaleciéndome con sus palabras para tomar un aliento mas de esfuerzo.

A mis abuelitos José, María - Pedro quienes han sido una parte esencial en mi vida y al igual les debo gran parte de la persona que soy, en especial a mi abuelita María Andrea Morales a quien le hubiera gustado mucho, verme terminar la carrera.

A mis tíos, primos y familia en general por sus consejos y cariño.

Con Amor

Adriana Lucía Morales Flores

DEDICATORIA

Dedico esta tesis, a Dios por guiar mis caminos y fortalecer mi vida ante todas las adversidades.

A dos seres maravillosos como son mis padres Hugo y Eugenia, quienes con amor, han trabajo y se han esforzado para dármelo todo, pendientes siempre de que mi formación personal e intelectual sean las mejores, apoyándome en cada momento para lograr culminar mis estudios universitarios. Son ellos quienes siempre han estado junto a mí, inculcándome valores, alentándome con sus palabras, entregándome sus consejos y sabiduría para que cada instante de mi vida sea mejor.

A mis hermanos Isabel y Diego, a mis primos Edison y Betty quienes son mi motivo de continuar adelante.

A aquella persona especial, quien desde el momento que llegó a formar parte de mi vida ha estado acompañándome y apoyándome, rompiendo cada barrera que se nos ha presentado, Roberto.

A dos ángeles que estoy segura desde el cielo están cuidándome y guiándome, siempre los llevaré en mi corazón Mamá Juanita y Lenin.

Dios los bendiga por todo.
Jeaneth Verónica Ruchi Yungán

ÍNDICE

CAPÍTULO 1 1
1.1 Descripción del Proyecto. 2
1.2 Características Generales de los Enrutadores Marca Cisco 5
1.2.1 Definición del Router 5
1.2.2 Funciones Básicas del Router 6
1.3 Componentes Básicos del Router 6
1.3.1 CPU: Unidad Central de Procesamiento 6
1.3.2 ROM: Memoria de solo Lectura 6
1.3.3 NVRAM: Memoria de Acceso Aleatorio no Volátil 7
1.3.4 Buses: 7
1.3.5 Interfaces: 7
1.3.6 Memoria Flash: 7
1.3.7 RAM: Memoria de Acceso Aleatorio 8
1.3.8 Fuente de Alimentación: 8
1.4 Modos de Configuración 9
1.4.1 Modo Usuario 9
1.4.2 Modo Privilegiado 9
1.4.3 Modo Configuración Global 9
1.4.4 Modo Configuración de Interfaces 9
1.4.5 Modo Configuración de Línea 9
1.4.6 Modo Configuración de Mantenimiento 10
1.5 Comandos Básicos para la Configiración de un Router 10

CAPÍTULO 2 11

2.1 Direccionamiento Ipv4 12
2.1.1 Dirección Ipv4 12
2.1.2 Encabezado de Ipv4 13
2.1.3 Clases de Redes 14
2.1.4 Subnetting 17
2.1.5 VLSM (Máscara de Subred de Tamaño Variable) 17
2.1.6 CIDR (Enrutamiento entre Dominios sin Clase) 18
2.1.7 Sumarización de Rutas 18
2.2 Consumo actual de Direcciones Ipv4 19
2.2.1 Disponible en IANA 19
2.2.2 Estado por /8 20
2.2.3 Disponible Histórico en IANA 20
2.2.4 Estado por RIR 21
2.2.5 Estado de las Direcciones Ipv4 22
2.3 Predicciones agotamiento del espacio de Direcciones Ipv4 23
2.4 IPv6 (Protocolo de Internet Versión 6) 24
2.4.1 Motivos de un Nuevo Protocolo 25
2.4.2 La Cabecera Ipv6 25
2.4.3 Partes de una Dirección Ipv6 27
2.5 Características Principales de Ipv6 28
2.6 Espacio de Direccionamiento Ipv6 30
2.6.2 Identificación de los Tipos de Direcciones 31
2.7 La Autoconfiguración en Ipv6 32
2.7.1 Tipos de Autoconfiguración 33

2.8 Enrutamiento con Ipv6 33
2.8.1 Enrutadores Ipv6 34
2.8.2 Tablas de Enrutamiento 35
2.9 Proceso de Solicitud de Direcciones Ipv6 36
2.9.1 IANA (Internet Assigned Number Authority) 37
2.9.2 Registro de Internet Regional (RIR) 37
2.9.3 LACNIC (Registro de Direcciones de Internet para América Latina y el Caribe) 38
2.9.4 Registro de Internet (IR) 38
2.9.5 Registro de Internet Nacional (NIR) 38
2.9.6 Registro de Internet Local (LIR) 38
2.9.7 Proveedor de Servicios de Internet (ISP) 39
2.9.8 Sitio Final o Usuario Final (EU) 39

CAPÍTULO 3 40
3.1 Funciones de la Capa de Red del Modelo OSI 41
3.2 IGP y EGP, protocolos enrutados y protocolos de enrutamiento 42
3.2.1 Protocolo Enrutado 42
3.2.2 Protocolo de Enrutamiento 42
3.3 Criterios de Selección de Protocolos de Enrutamiento 47
3.4 BGP (Border Gateway Protocol) 48
3.4.1 Tipos de Mensajes BGP 49
3.5 iBGP y ebgp 50
3.5.1 eBGP 50
3.5.2 iBGP 51
3.6 Atributos de la Ruta de Acceso 52
3.6.1 Categorías de los Atributos en BGP 53
3.7 Selección de Ruta y Manipulación de Atributos 55
3.7.1 Selección de Ruta 56
3.7.2 Manipulación de Atributos en BGP 59
3.8 BGP con IPv6 63
3.9 Comandos de Configuración de BGP sobre Equipamiento Marca Cisco 64

CAPÍTULO 4 65
4.1 Mecanismos de Transición de IPv4 a IPv6 66
4.1.1 Mecanismo Doble Pila (Ipv4 a Ipv6) 67
4.1.2 Mecanismo de Túnel 68
4.2.3 Mecanismos de Traducción 72
4.2 Mecanismo que Mejor se Adapta a BGP 73
4.3 Comandos de configuración Ipv6 sobre Equipamiento Marca Cisco 74

CAPÍTULO 5 75
5.1 Topología de la Red 77
5.1.1 NAP 79
5.2 Enrutamiento y Tráfico 79
5.2.1 Enrutamiento 79
5.2.2 Peering (Intercambio de Tráfico) 80
5.2.3 Monitoreo de Tráfico - NAP.EC 82

5.3 Políticas de Seguridad, Peering y Enrutamiento..... 83
5.3.1 Políticas de Seguridad..... 83

CAPÍTULO 6..... 86
6.1 Software de Simulación..... 87
6.1.1 Introducción..... 87
6.1.2 GNS3 (Simulador de Red Gráfico)..... 88
6.1.3 Aplicación..... 89
6.1.4 Utilización de recursos..... 89
6.1.5 Imágenes IOS..... 90
6.2 Topología de la Red Simulada..... 91
6.3 Asignación de Direcciones IPv6..... 92
6.3.1 Asignación a la infraestructura del operador..... 92
6.3.2 Asignaciones directas a Usuarios Finales..... 92
6.3.3 Microasignación en IPv6..... 94
6.3.4 Registro..... 95
6.3.5 Resolución inversa..... 96
6.3.6 Poseedores de IPv6 ya existentes..... 96
6.4 Configuraciones del Equipamiento Simulado..... 96
6.4.1 Configuración del router 1 (QUITO)..... 96
6.4.2 Configuración del router 2 (GUAYAQUIL)..... 102
6.4.3 Configuración del router 3 (TE UNO)..... 107
6.4.4 configuración del router 4 (TELMEX)..... 109
6.4.5 configuración del router 5 (ECUANET)..... 111
6.4.6 configuración del router 6 (PORTA)..... 113
6.5 Comprobación de la Operación del Protocolo de Enrutamiento y del Cumplimiento de Políticas..... 115
6.5.1 Comprobación del Protocolo de Enrutamiento..... 115
6.5.2 Cumplimiento de Políticas..... 116

CAPÍTULO 7..... 121
7.2 Requerimientos de Hardware y Software..... 122
7.2.1 Requerimientos de hardware..... 122
7.2.2 Requerimientos de software..... 124
7.3 Costos nuevos requerimientos de hardware..... 126
7.4 Costos de software y direcciones Ipv6..... 126
7.4.1 Costo de software..... 126
7.4.2 Costo de direcciones IPv6..... 126
7.5 Análisis Costo – Beneficio..... 127
7.5.1 Análisis de Costos..... 127
7.5.2 Indicadores de Rentabilidad..... 130
7.5.3 Relación Beneficio Costo (C/B)..... 132
7.6 Recuperación de la Inversión..... 133
7.6.1 Periodo de Recuperación de la Inversión (PRI)..... 133

ÍNDICE DE FIGURAS

FIGURA 1.1 Router y una conexión a Internet 5
FIGURA 1.2 Componentes básicos del Router 8
FIGURA 2.1 Direccionamiento IPv4 12
FIGURA 2.2 El encabezado de IPv4 13
FIGURA 2.3 Clases de Direcciones IP 14
FIGURA 2.4 Dirección IP Clase A 15
FIGURA 2.5 Dirección IP Clase B 15
FIGURA 2.6 Dirección IP Clase C 16
FIGURA 2.7 Dirección IP Clase D 16
FIGURA 2.8 Distribución de direcciones IPv4 19
FIGURA 2.9 Estado del Pool de direcciones IPv4 19
FIGURA 2.10 Estado de direcciones Ipv4 20
FIGURA 2.11 Estado del IANA 20
FIGURA 2.12 Estado por RIR 21
FIGURA 2.13 Estado del Pool de Direcciones 22
FIGURA 2.14 Estimación según Geoff Huston 23
FIGURA 2.15 Encabezado fijo de IPv6 26
FIGURA 2.16 Formato de direcciones IPv6 27
FIGURA 2.17 Direccionamiento Unicast 30
FIGURA 2.18 Direccionamiento Anycast 30
FIGURA 2.19 Direccionamiento Multicast 31
FIGURA 2.20 Enrutamiento IPv6 34
FIGURA 2.21 Registros de Internet Regionales 36
FIGURA 3.1 Conexión entre Sistemas Autónomos 43
FIGURA 3.2 Conexión de dos redes mediante BGP 48
FIGURA 3.3 iBGP vs. eBGP 50
FIGURA 3.4 Formato del tipo de atributo de ruta de acceso 52
FIGURA 3.5 Visión general del proceso de enrutamiento 57
FIGURA 4.1 Mecanismo Doble Pila 67
FIGURA 4.2 Mecanismo de Túnel 68
FIGURA 4.3 Túnel 6to4 69
FIGURA 4.4 Conexión mediante Toredo 70
FIGURA 4.5 Conexión mediante Túnel Broker 71
FIGURA 4.6 Mecanismo de Traducción 72
FIGURA 5.1 Nodos de Intercambio de Tráfico en Ecuador 77
FIGURA 5.2 Topología del NAP 78
FIGURA 6.1 Logo del software de simulación 88
FIGURA 6.2 Topología de la red simulada 91
FIGURA 6.3 Protocolo de enrutamiento BGP 116
FIGURA 6.4 IPv6 116
FIGURA 6.5 Sesión BGP 117
FIGURA 6.6 IPv6 117
FIGURA 6.7 Bloqueo de Redes privadas y experimentales 118
FIGURA 6.8 IPv6 118
FIGURA 6.9 Bloqueo de prefijos com máscara de más de 24 bits 119
FIGURA 6.10 IPv6 119
FIGURA 6.11 Verificación del Atributo MED 120
FIGURA 6.12 IPv6 120
FIGURA 7.1 Plataforma del IOS de Cisco 125

ÍNDICE DE TABLAS

Tabla 7.1 Equipos de NAP.EC 127
Tabla 7.2 Costo de Software 127
Tabla 7.3 Costos de Capacitación 128
Tabla 7.4 Gastos Administrativos 128
Tabla 7.5 Costos de Implementación 129
Tabla 7.6 Flujo Neto del proyecto 129
Tabla 7.7 Valores para calcular el VAN 131
Tabla 7.8 Datos para calcular el PRI 133

RESUMEN

Cuando se diseñó el actual Protocolo Internet (IP versión 4), en los años setenta, no se podía prever el enorme crecimiento de Internet. Actualmente, no existen suficientes direcciones IP hecho de que no haya suficiente espacio de direccionamiento IPv4 está ocasionando que muchos países como Japón y los países de África y Latinoamérica tengan restricciones en el acceso a Internet, a los servicios y aplicaciones de nueva generación.

Las redes inalámbricas de celulares donde cada dispositivo tiene una dirección IP serian imposibles sin IPv6, por ejemplo solo en Ecuador hay cerca de 10 millones de celulares, mientras hay solo 4 millones de direcciones IPv4.

Muchos Proveedores de Servicios de Internet (ISPs) a nivel global ya cuentan con sus troncales preparadas para la demanda de clientes que quieran desplegar el nuevo protocolo.

En cuanto al intercambio de tráfico, varios NAPs de la región han implementado el protocolo y ofrecen a quienes son sus miembros intercambiar prefijos IPv6 además de IPv4.

Dado que IPv6 es un protocolo nuevo, no es compatible con IPv4, y por ello IPv6 ha sido diseñado previendo un largo período de transición y co-existencia entre ambos.

Este proyecto tiene como fin realizar un estudio para la transición IPv4 a IPv6 de una infraestructura de Internet que utiliza BGP como protocolo de enrutamiento, basándonos en las restricciones y características propias del NAP.EC.

PRESENTACIÓN

Para un mejor desarrollo a la tesis se le ha dividido en 7 capítulos, los mismos que han sido desarrollados como se muestra a continuación.

CAPÍTULO I: Este capitulo trata sobre una breve descripción del proyecto y características generales de los enrutadores marca Cisco.

CAPÍTULO II: En este capitulo, se detallará los fundamentos teóricos proporcionando amplia información del protocolo IPv4 (consumo actual, clases, subneting, VLSM, CIDR, sumarización, predicción de agotamiento del espacio de direcciones). En lo que se refiere al protocolo IPv6 (características principales, direccionamiento, enrutamiento, autoconfiguración).

CAPÍTULO III: En este capítulo describe los conceptos básicos de BGP, funciones del modelo OSI, IGP, EGP, atributos de la ruta de acceso, selección de rutas y manipulación de atributos.

CAPÍTULO IV: Este capítulo aporta información sobre el proceso de transición de IPv4 a IPv6 y mecanismos que mejor se adaptan a BGP.

CAPÍTULO V: En este capítulo, se explica el análisis de la situación actual de la red, topología de la red, enrutamiento, tráfico, políticas de seguridad y peering.

CAPÍTULO VI: Este capítulo, cubre la simulación del escenario planteado mediante un software y configuraciones del equipamiento a utilizarse, verificándose la correcta operación de los protocolos.

CAPÍTULO 1.

INTRODUCCIÓN

En este primer capítulo esta dedicado a dar una teoría introductoria sobre la descripción del proyecto, además tratará sobre los enrutadores marca cisco (definición, componentes básicos, modos de configuración entre otros).

1.1 DESCRIPCIÓN DEL PROYECTO

El reducido espacio de Ipv4, a pesar de disponer de más de cuatro mil millones de direcciones (4.294.967.298) junto al hecho de una importante falta de coordinación, durante la década de los 70, en la delegación de direcciones, sin ningún tipo de optimización, dejando incluso grandes espacios discontinuos, nos está llevando a límites no sospechados en aquel momento por lo que se ve necesario la adquisición de un nuevo protocolo como es IPv6.

Por supuesto, hay una solución que se podría considerar como evidente, como sería la remuneración y reasignación de dicho espacio de direccionamiento. Sin embargo, no es tan sencillo, es incluso impensable en algunas redes, ya que requiere unos esfuerzos de coordinación, a escala mundial, absolutamente impensables.

A medida que la población mundial crece, se hace necesario planificar la posibilidad de que todas las personas puedan acceder a Internet. Cuando se diseñó el actual Protocolo Internet (IP versión 4), en los años setenta, no se podía prever el enorme crecimiento de Internet. Actualmente, no existen suficientes direcciones IP para todos los habitantes del planeta, la falta de direcciones no es apreciable por igual en todos los puntos de la red, de hecho, no es casi apreciable, por el momento en Norte América. El hecho de que no haya suficiente espacio de direccionamiento IPv4 está ocasionando que muchos países como Japón y los países de África y Latinoamérica tengan restricciones en el acceso a Internet, a los servicios y aplicaciones de nueva generación.

Tanto en Japón como en Europa el problema es creciente, dado el importante desarrollo de las redes de telefonía celular, inalámbricas, módems de cable, xDSL, etc., que requieren direcciones IP fijas para aprovechar al máximo sus

posibilidades e incrementar el número de aplicaciones en las que pueden ser empleados.

Las redes inalámbricas de celulares donde cada dispositivo tiene una dirección IP serian imposibles sin IPv6, por ejemplo solo en Ecuador hay cerca de 10 millones de celulares, mientras hay solo 4 millones de direcciones IPv4. No quiere decir que las redes móviles de la nueva generación sean la única aplicación de IPv6, ni la más importante, pero si esta dentro del grupo de las que se pueden considerar como las más importantes.

Se encuentran hoy realizando la transición hacia una actualización del protocolo de Internet que ha estado utilizando en los últimos años. Y más allá de las cuestiones técnicas que aún merezcan o no un mayor debate, lo cierto es que IPv6 se está implementando en el mundo y que las estadísticas muestran que el cambio se hace necesario.

Muchos Proveedores de Servicios de Internet (ISPs) a nivel global ya cuentan con sus troncales preparadas para la demanda de clientes que quieran desplegar el nuevo protocolo. En cuanto al ambiente académico la realidad es más alentadora, ya que desde hace muchos años este sector ha estado trabajando, investigando e implementando IPv6, habiéndose convertido en los primeros en demandar el servicio que hoy se ha hecho extensivo a la comunidad en general.

En cuanto al intercambio de tráfico, varios NAPs de la región han implementado el protocolo y ofrecen a quienes son sus miembros intercambiar prefijos IPv6 además de IPv4. Esto, más allá de la cuestión técnica del intercambio de prefijos, ayuda a que los ISPs y miembros de NAPs se interesen en el tema y planifiquen su implementación.

Dado que IPv6 es un protocolo nuevo, no es compatible con IPv4, y por ello IPv6 ha sido diseñado previendo un largo período de transición y co-existencia entre ambos. Es difícil concretar durante cuánto tiempo ambos protocolos seguirán siendo utilizados y en que momento prácticamente se dejara de utilizar IPv4, dado

que depende de muchos factores, tanto técnicos como comerciales. Desde un punto de vista técnico se puede afirmar que la transición se puede hacer prácticamente sin ayuda de los ISPs, teniendo en cuenta que los sistemas operativos, desde el año 2001, ya incorporan IPv6 y mecanismos de transición automáticos.

Pero esta transición puede ser más eficaz si se implican los ISPs lo antes posible, lo que además, a la larga, les facilitará el ofrecer nuevos servicios y aplicaciones, ofrecer mejor calidad de servicio a los usuarios e incluso podría reducir algunos de los costes de los ISPs.

Este proyecto tiene como fin realizar un estudio para la transición IPv4 a IPv6 de una infraestructura de Internet que utiliza BGP como protocolo de enrutamiento, basándonos en las restricciones y características propias del NAP.EC.

Se realizará una simulación del escenario planteado en la que verifique la correcta operación de los protocolos (de enrutamiento y enrutados), para esto se utilizará un software que incluye un ambiente gráfico para la creación de topología de redes y un emulador de hardware de enrutadores.

Por último, se realizará un análisis para determinar el presupuesto en el que incurriría la administración del NAP al implementar este nuevo soporte.
No es parte del proyecto la implementación del mismo, esto lo realizara AEPROVI conforme lo considere necesario.

La tesis se ha desarrollado de tal forma que el lector pueda adentrarse en los conceptos teóricos determinando los requerimientos técnicos, económicos que envuelven a un problema de esta índole y posteriormente pueda seguir paso a paso las configuraciones de software requeridas, por último se comprobará mediante una simulación la configuración del equipamiento.

1.2 CARACTERÍSTICAS GENERALES DE LOS ENRUTADORES MARCA CISCO

1.2.1 DEFINICIÓN DE ROUTER

Es un dispositivo de red que permite el enrutamiento de paquetes entre redes independientes. Este enrutamiento se realiza de acuerdo a un conjunto de reglas que forman la tabla de enrutamiento.

Es un dispositivo que opera en la capa 3 del modelo OSI. Los enrutadores se utilizan para conectar varias redes. Por ejemplo, puede utilizar para conectar sus computadoras en red a Internet y, de esta forma, compartir una conexión de Internet entre varios usuarios. Como se observa en la Figura 1.1 el router actuará como distribuidor, seleccionado la mejor ruta de desplazamiento de la información para que la reciba rápidamente.

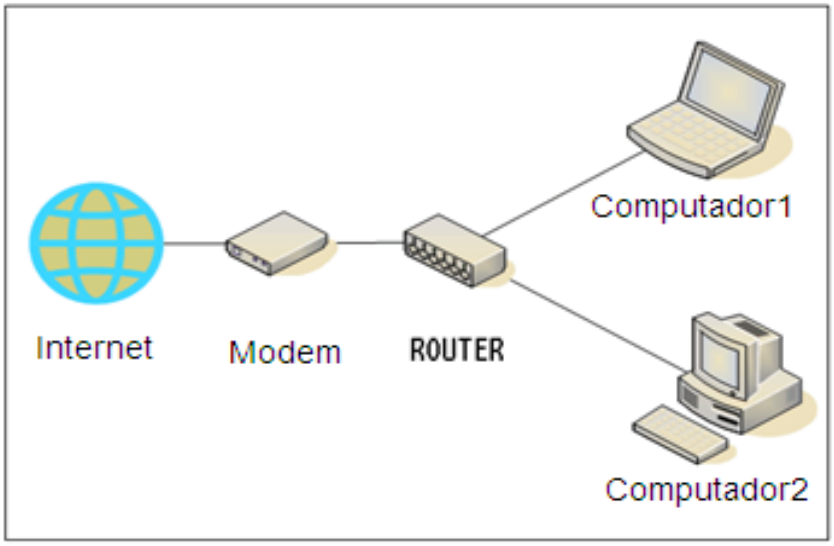


FIGURA 1.1 Router y una conexión a Internet

Los enrutadores analizan los datos que se van a enviar a través de una red, los empaquetan de forma digerente y los envían a otra red a través de un tipo de red distinto. Conectan una red con el mundo exterios, incluso, pueden decidir qué computadoras tienen prioridad sobre las demás.

1.2.2 FUNCIONES BÁSICAS DEL ROUTER

El ruteador es el responsable de crear y mantener tablas de ruteo, estas tablas son creadas ya sea estáticamente o dinámicamente. De esta manera el ruteador extrae de la capa de red la dirección destino y realiza una decisión de envío basado sobre el contenido de la especificación del protocolo en la tabla de ruteo.

La inteligencia de un ruteador permite seleccionar la mejor ruta, basándose sobre diversos factores, más que por la dirección MAC[1] destino. Estos factores pueden incluir la cuenta de saltos, velocidad de la línea, costo de transmisión, retraso y condiciones de tráfico.

1.3 COMPONENTES BÁSICOS DEL ROUTER

1.3.1 CPU: UNIDAD CENTRAL DE PROCESAMIENTO

Ejecuta las instrucciones del sistema operativo. Estas funciones incluyen la inicialización del sistema, enrutamiento y el control de la interfaz de red.

1.3.2 ROM: MEMORIA DE SOLO LECTURA

Se utiliza para almacenar de forma permanente el código de diagnóstico de inicio (Monitor de ROM). Las tareas principales de la ROM son el diagnóstico del hardware durante el arranque del router y la carga del software IOS[2] de Cisco desde la memoria flash a la RAM.

---

1. **(Media Access Control - Control de Acceso al Medio).** Es un identificador único en el mundo representado en notación hexadecimal y conformado por 48 bits. Dicho identificador se asigna a las tarjetas de red.

2. **(Internetwork Operating System - Sistema Operativo de Interconexión de Redes)** sistema operativo creado por Cisco System para programar y mantener equipos de interconexión de redes informáticas como switches (conmutadores) y routers (enrutadores).

1.3.3 NVRAM: MEMORIA DE ACCESO ALEATORIO NO VOLÁTIL

Guardar la configuración de inicio. En algunos dispositivos, la NVRAM se implementa utilizando distintas memorias de solo lectura programables, que se pueden borrar electrónicamente (EEPROM)[3].

En otros dispositivos, se implementa en el mismo dispositivo de memoria flash desde donde se cargó el código de arranque.

En cualquiera de los casos, estos dispositivos retienen sus contenidos cuando se apaga la unidad

1.3.4 BUSES

La mayoría de los enrutadores contienen un bus de sistema y un bus de CPU. El bus de sistema se usa para la comunicación entre la CPU y las interfaces y/o ranuras de expansión. Este bus transfiere los paquetes hacia y desde las interfaces.

1.3.5 INTERFACES

Las interfaces son las conexiones de los enrutadores con el exterior. Los tres tipos de interfaces son la red de área local (LAN), la red de área amplia (WAN) y la Consola/AUX.

1.3.6 MEMORIA FLASH

La memoria flash se utiliza para almacenar una imagen completa del software IOS de Cisco.

---

3. Conocida también como E²PROM son las siglas de (Electrically Erasable Programmable Read Only Memory - ROM programable y borrable eléctricamente). Es un tipo de memoria ROM que puede ser programado, borrado y reprogramado eléctricamente.

1.3.7 RAM: MEMORIA DE ACCESO ALEATORIO

Se usa para la información de las tablas de enrutamiento, caché de conmutación rápida, la configuración actual y las colas de paquetes. En la mayoría de los enrutadores, la RAM proporciona espacio de tiempo de ejecución para el software IOS de Cisco y sus subsistemas. Ver Figura 1.2. Fuente de alimentación Ventilador RAM no volátil (NVRAM).

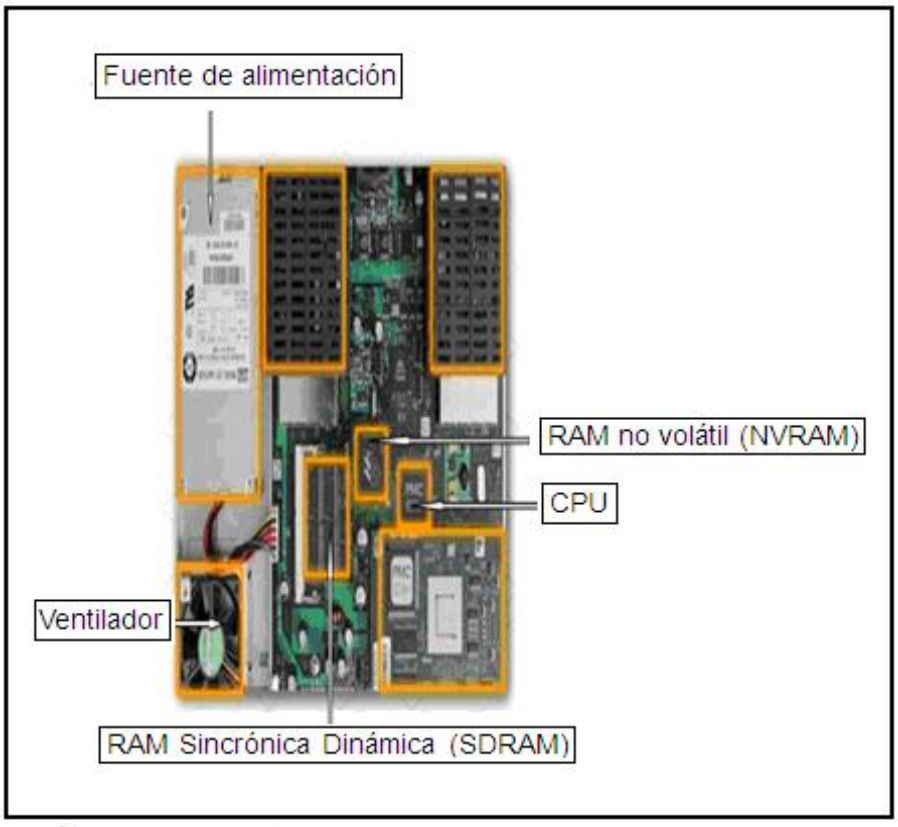


FIGURA 1.2 Componentes básicos del Router

1.3.8 FUENTE DE ALIMENTACIÓN

Está fuente brinda la energía necesaria para operar los componentes internos. Los enrutadores de mayor tamaño pueden contar con varias fuentes de alimentación o fuentes modulares. En algunos de los enrutadores de menor tamaño, la fuente de alimentación puede ser externa al router.

1.4 MODOS DE CONFIGURACIÓN

1.4.1 MODO USUARIO

Permite consultar toda la información relacionada al router sin poder modificarla. El shell es el siguiente:

Router >

1.4.2 USUARIO PRIVILEGIADO

Permite visualizar el estado del router e importar o exportar imágenes de IOS. El shell es el siguiente:

Router #

1.4.3 MODO DE CONFIGURACIÓN GLOBAL

Permite utilizar los comandos de configuración generales del router. El shell es el siguiente:

Router (config) #

1.4.4 MODO DE CONFIGURACIÓN DE INTERFACES

Permite utilizar comandos de configuración de interfaces (Direcciones IP, mascaras, etc.). El shell es el siguiente:

Router (config-if) #

1.4.5 MODO DE CONFIGURACIÓN DE LÍNEA

Permite configurar una línea (consola o línea virtual). El shell es el siguiente:

Router (config-line) #

1.4.6 MODO DE MANTENIMIENTO

Modo de mantenimiento que puede servir, especialmente, para reinicializar las contraseñas del router. El shell es el siguiente:

rommon >

1.5 COMANDOS BÁSICOS PARA LA CONFIGURACIÓN DE UN ROUTER

En el Anexo 1, se muestra los comandos básicos para configurar un router.

CAPÍTULO 2.

IPV6 (PROTOCOLO DE INTERNET VERSIÓN 6)

En este capítulo, se tratará todo lo concerniente a direccionamiento IPv4 (concepto, clases, subnetting, máscara de subred de tamaño variable, enrutamiento inter-dominios sin clases, consumo actual, entre otros); así como la estructura de su encabezado de red. Se realiza una introducción al protocolo de Internet versión 6 comparando las diferencias que existen entre este encabezado y el de IPv4. Así mismo, se hace una descripción de la nueva notación de direcciones IP utilizadas por esta versión.

2.1 DIRECCIONAMIENTO IPv4

2.1.1 DIRECCIÓN IP

La dirección IP es un número único que identifica a una computadora o dispositivo conectado a una red que se comunica a través del protocolo de redes TCP/IP, este se relaciona automáticamente como el protocolo sobre el que funciona la red Internet.

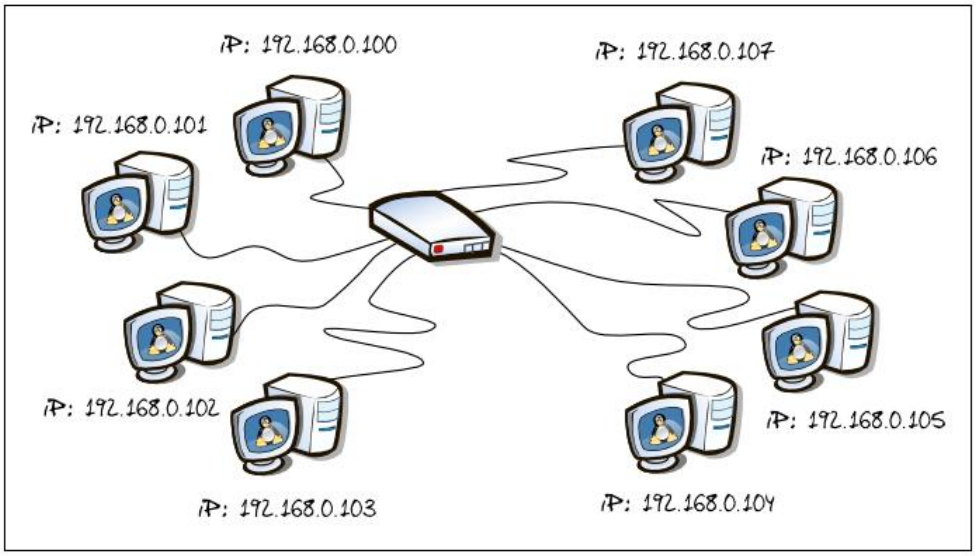


FIGURA 2.1 Direccionamiento IPv4

El protocolo TCP (Protocolo de Control de Transmisión), funciona en el nivel de transporte del modelo de referencia OSI, proporcionando un transporte fiable de datos.

El protocolo IP (Protocolo de Internet), funciona en el nivel de red del modelo OSI, que permite encaminar los datos hacia otras máquinas.

Todas las direcciones IPv4 son de 32 bits de longitud y se usan en los campos de Dirección de Origen y de Dirección de Destino de los paquetes IP. Estás direcciones están compuestas por cuatro números enteros (4 bytes), es decir, cuatro grupos de 8 bits cada uno (xxxx.xxxx.xxxx.xxxx), cada segmento de 8 bits varía de 0-255 y están separados por un punto, por ejemplo esta es una dirección IP en formato técnico: 194.153.205.26. Ver Figura 2.1.

2.1.2 ENCABEZADO DEL IPv4

La versión IPv4, que es utilizada actualmente en las redes a nivel mundial, el encabezado presenta el formato que se muestra en la Figura 2.2.

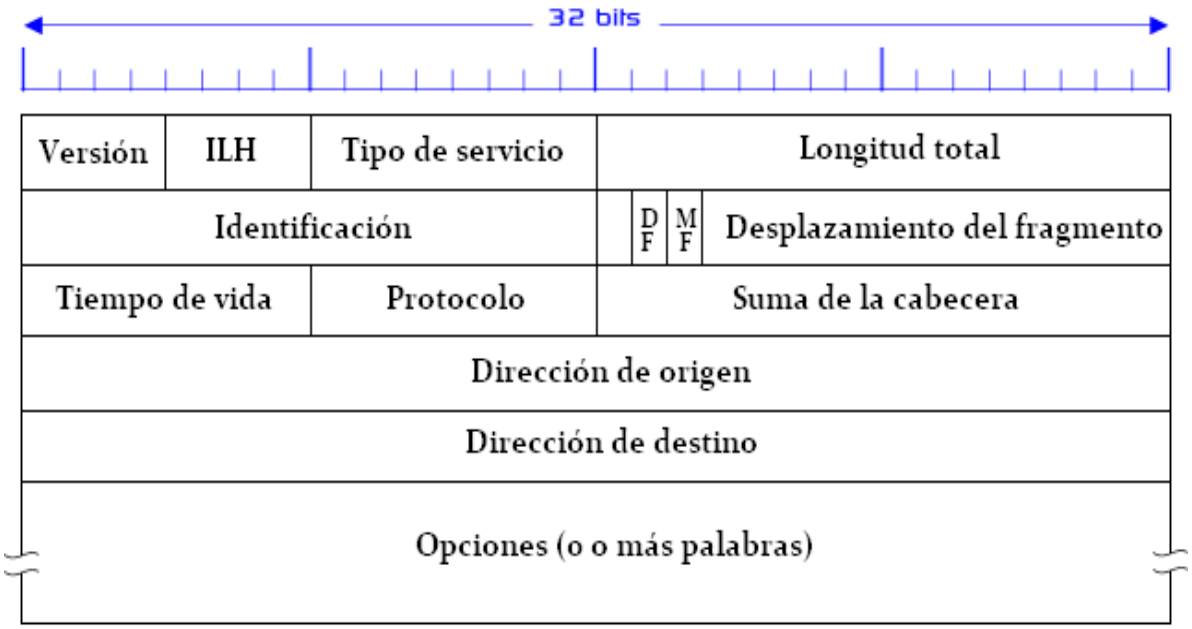


FIGURA 2.2 El encabezado de IPv4

El organismo no lucrativo a cargo de asignar direcciones públicas de IP, desde 1998 es IANA (Agencia de Asignación de Números de Internet). La estructura jerárquica de estos organismos será analizada más adelante en el tema Proceso de solicitud de direcciones IPv6.

Por varias décadas, las direcciones IP se dividieron en cinco categorías, las cuales se listan en la Figura 2.3. Esta asignación se ha llamado Direccionamiento con Clase. La cual ya no se utiliza, pero en la literatura aún es común encontrar referencias.

2.13 CLASES DE REDES

El objetivo de dividir las direcciones IP en clases es facilitar la búsqueda de un equipo en la red. De hecho, con esta notación es posible buscar primero la red a la que uno desea tener acceso y luego buscar el equipo dentro de esta red.

Puesto que en Internet coexisten muchos tipos de redes, para dotar de flexibilidad al sistema, se dispuso que existieran cinco modelos o clases distintas de direcciones: **A**, **B**, **C**, **D** y **E**. Dicho de otro modo: el espacio total de direcciones posibles se dividió en cinco categorías o clases predefinidas, como mencionamos anteriormente.

FIGURA 2.3 Clases de Direcciones IP

2.1.3.1 CLASE A

Admite redes de tamaño extremadamente grande. Este tipo de direcciones comienzan con 0, lo que significa que hay 2^7 = 128 posibilidades de red, el mismo que va entre 1 y 126.

Como se muestra en la Figura 2.4, los tres últimos octetos son asignados a los hosts, de modo que la cantidad máxima de hosts es $2^{24} - 2^1 = 16\ 777\ 214$ equipos.

FIGURA 2.4 Dirección IP Clase A

La red 127.0.0.0 se reserva para las **pruebas de loopback**[4]. Por lo tanto, no se puede asignar este número a una red.

2.1.3.2 CLASE B

Cumplen las necesidades de redes de tamaño moderado a grande. Los primeros dos bits son 1 y 0; esto significa que existen $2^{14} = 16.384$ posibilidades de red. Las redes de la clase B son, por lo tanto, redes que van de 128.0.0.0 a 191.255.0.0.

Los dos bytes de la izquierda representan los equipos de la red. La red puede entonces contener una cantidad de equipos equivalente a: $2^{16}-2^1 = 65.534$ equipos. Ver Figura 2.5.

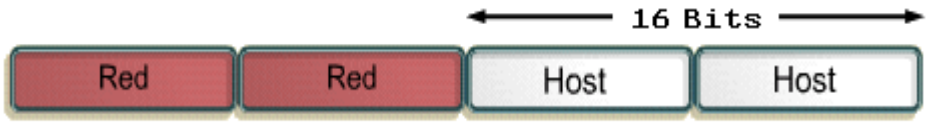


FIGURA 2.5 Dirección IP Clase B

2.1.3.3 CLASE C

Admitir redes pequeñas. Los primeros tres bits son 1,1 y 0; esto significa que hay 2^{21} posibilidades de red, es decir, 2.097.152. Las redes disponibles de la clases C son, por lo tanto, redes que van desde 192.0.0.0 a 223.255.255.0.

---

4. Se utilizan a menudo para probar la disponibilidad de la interfaz de red.

Al observar la Figura 2.6, se ve que el byte de la derecha representa los equipos de la red, por lo que la red puede contener: 2^8-2^1 = 254 equipos.

FIGURA 2.6 Dirección IP Clase C

2.1.3.4 CLASE D

La dirección Clase D se creó para permitir multicast en una dirección IP. Ver Figura 2.7. Una dirección multicast es una dirección exclusiva de red que dirige los paquetes con esa dirección destino hacia grupos predefinidos de direcciones IP.
Por lo tanto, una sola estación puede transmitir de forma simultánea una sola corriente de datos a múltiples receptores. Los primeros cuatro bits de una dirección de este tipo deben ser 1110. Por lo tanto, el primer rango de octeto para las direcciones Clase D es 224 a 239.

FIGURA 2.7 Dirección IP Clase D

2.1.3.5 CLASE E

Se ha definido una dirección Clase E. Sin embargo, la Fuerza de Tareas de Ingeniería de Internet (IETF) ha reservado estas direcciones para su propia investigación.

Por lo tanto, no se han emitido direcciones de esta Clase para ser utilizadas en Internet. Los primeros cuatro bits de dicha dirección siempre son 1s. Por lo tanto, el rango del primer octeto para las direcciones Clase E es 240 a 255.

2.1.4 SUBNETTING

La función del Subneteo o Subnetting es dividir una red IP redes más pequeñas para que cada una de estas trabaje a nivel envío y recepción de paquetes como una red individual.

El Subneteo permite una mejor administración, control del tráfico y seguridad al segmentar la red por función. También, mejora el desempeño de la red al reducir el tráfico de broadcast[5] de nuestra red. Como desventaja, su implementación desperdicia muchas direcciones, sobre todo en los enlaces seriales.

2.1.5 VLSM (MÁSCARA DE SUBRED DE TAMAÑO VARIABLE)

Técnica que permite dividir subredes en redes fijas más pequeñas, luego se toma una de esas subredes y se vuelve a dividir tomando bits “prestados” de la porción de hosts, ajustándose a la cantidad de host requeridos por cada segmento de la red.

La regla que hay que tener en consideración siempre que se utilice VLSM es que solamente se puede aplicar esta técnica a las direcciones de redes/subredes que no están siendo utilizadas por ningún host, VLSM permite crear subredes más pequeñas que se ajusten a las necesidades reales de la red.

VLSM representan otra de las tantas soluciones que se implementaron para el agotamiento de direcciones IP y otras como la división en subredes, el enrutamiento de Interdominio CIDR, NAT[6] y las direcciones IP privadas.

---

5. Modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de producir la misma transmisión nodo por nodo.

6. (Network Address Translation – Traducción de Dirección de Red).- mecanismo utilizado por enrutadores IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles.

2.1.6 CIDR (ENRUTAMIENTO ENTRE DOMINIOS SIN CLASE)

Es la última actualización al método de interpretación de direcciones dentro de una red. CIDR es una medida para evitar problemas de crecimiento de las tablas y un mejor aprovechamiento de las direcciones IP.

Las direcciones IPs originales están delimitadas por cuatro segmentos denominados Octetos. Las direcciones IPs sin CIDR solo pueden identificar redes por segmentos de 8, 16 y 24.

CIDR es un sustituto para el proceso de asignación de direcciones de clase A, B y C, no se limita a los identificadores por segmentos sino que utiliza prefijos desde los 13 a los 27 bits.

Con este nuevo proceso se consigue que la asignación de direcciones sea más precisa y adecuada para las necesidades específicas de la empresa. Una dirección en formato CIDR consta de una dirección de IP más un sufijo que indica la cantidad longitud en bits del prefijo. Ejemplo: 192.168.68.0 / 14

El enrutamiento entre dominios sin clase es una técnica soportada por BGP y basada en el agregado de rutas. CIDR permite que los routers agrupen rutas para reducir la cantidad de información de enrutamiento transportada por los routers principales. Con CIDR, un conjunto de redes IP aparecen ante las redes que están fuera del grupo como una entidad única de mayor tamaño.

2.1.7 SUMARIZACIÓN DE RUTAS

También llamado resumen de ruta, supernetting o superredes, es el proceso realizado por un router a través de un protocolo de enrutamiento por el cual partiendo de un conjunto de direcciones de red (bloques CIDR) se obtiene una única dirección común que contiene a las demás para ser enviada en sus actualizaciones

2.2 CONSUMO ACTUAL DE DIRECCIONES IPV4.

El conjunto de direcciones IP de acuerdo a la tecnología IPv4 está distribuida en este momento de acuerdo a la siguiente grafica mostrada (Figura 2.8).

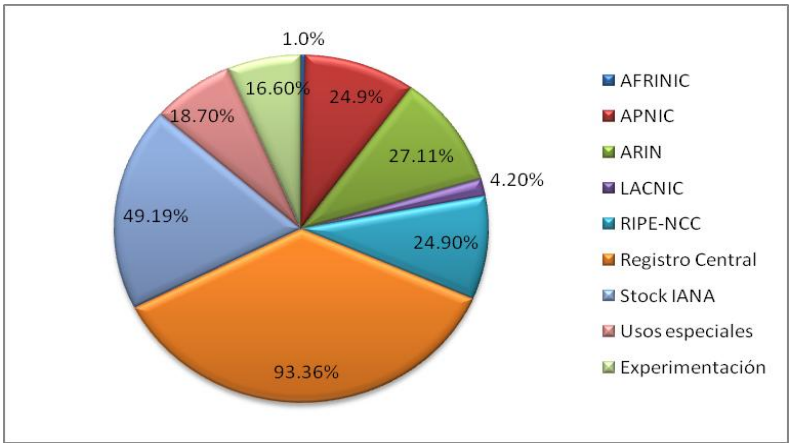


FIGURA 2.8 Distribución de direcciones IPv4
FUENTE: http://www.potaroo.net/tools/ipv4

2.2.1 DISPONIBLE EN IANA.

El espacio de direccionamiento IPv4 es de 32 bits, lo equivale a 256 bloques /8. Aproximadamente, 36 bloques /8 corresponden a direcciones reservadas (privadas), más de 219 bloques /8 para uso en el internet público IPv4. Al 14/08/09 quedan únicamente 26 bloques /8 en el pool de IANA. Ver Figura 2.9.

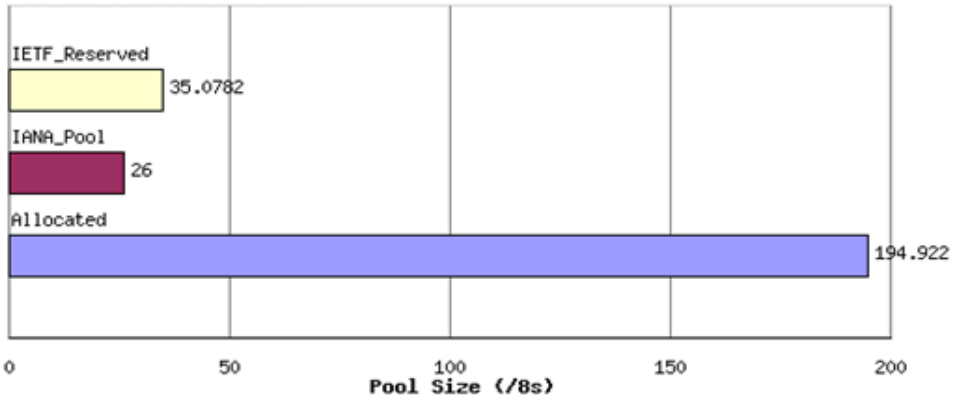


FIGURA 2.9 Estado del Pool de direcciones IPv4
FUENTE: http://www.potaroo.net/tools/ipv4

2.2.2 ESTADO POR /8.

Los pools de dirección se dan mediante la agrupación de espacio de direcciones en una secuencia de /8s, y mirando a sub totales dentro de cada Estado /8 bloque de direcciones. La Figura 2.10, muestra el estado actual del espacio de direcciones IPv4 como 256 /8 columnas, cada una describiendo un conjunto de 16.777.216 direcciones.

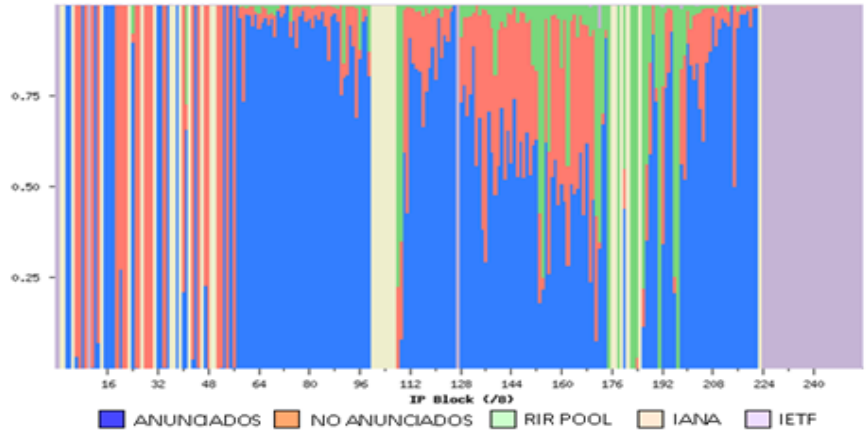


FIGURA 2.10 Estado de direcciones Ipv4
FUENTE: http://www.potaroo.net/tools/ipv4

2.2.3 DISPONIBLE HISTÓRICO EN IANA.

En la Figura 2.11, se ve que desde el año 2000 el stock estaba en un porcentaje del 103% y que año tras año ha ido disminuyendo hasta saber que hoy en día el stock central de direcciones del IANA se encuentra en un 30%.

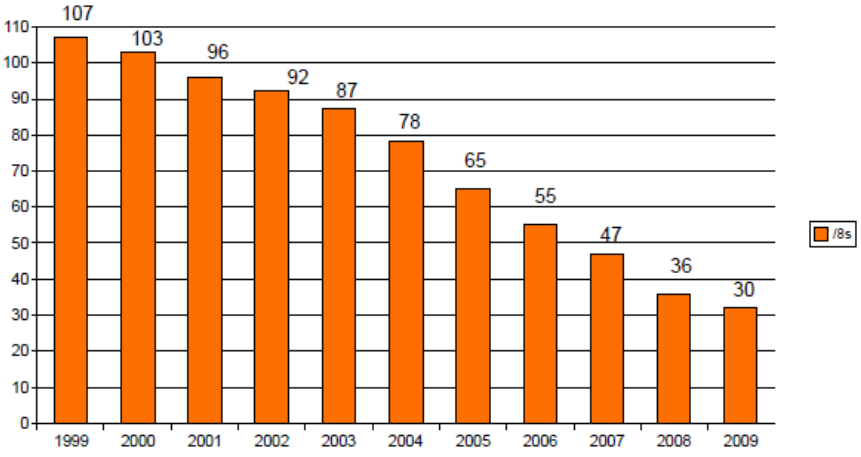


FIGURA 2.11 Estado del IANA

2.2.4 ESTADO POR RIR.

En la Figura 2.12 se muestra un cuadro estadístico de la clasificación del estado de direcciones IPv4 por tipos de interés comerciales.

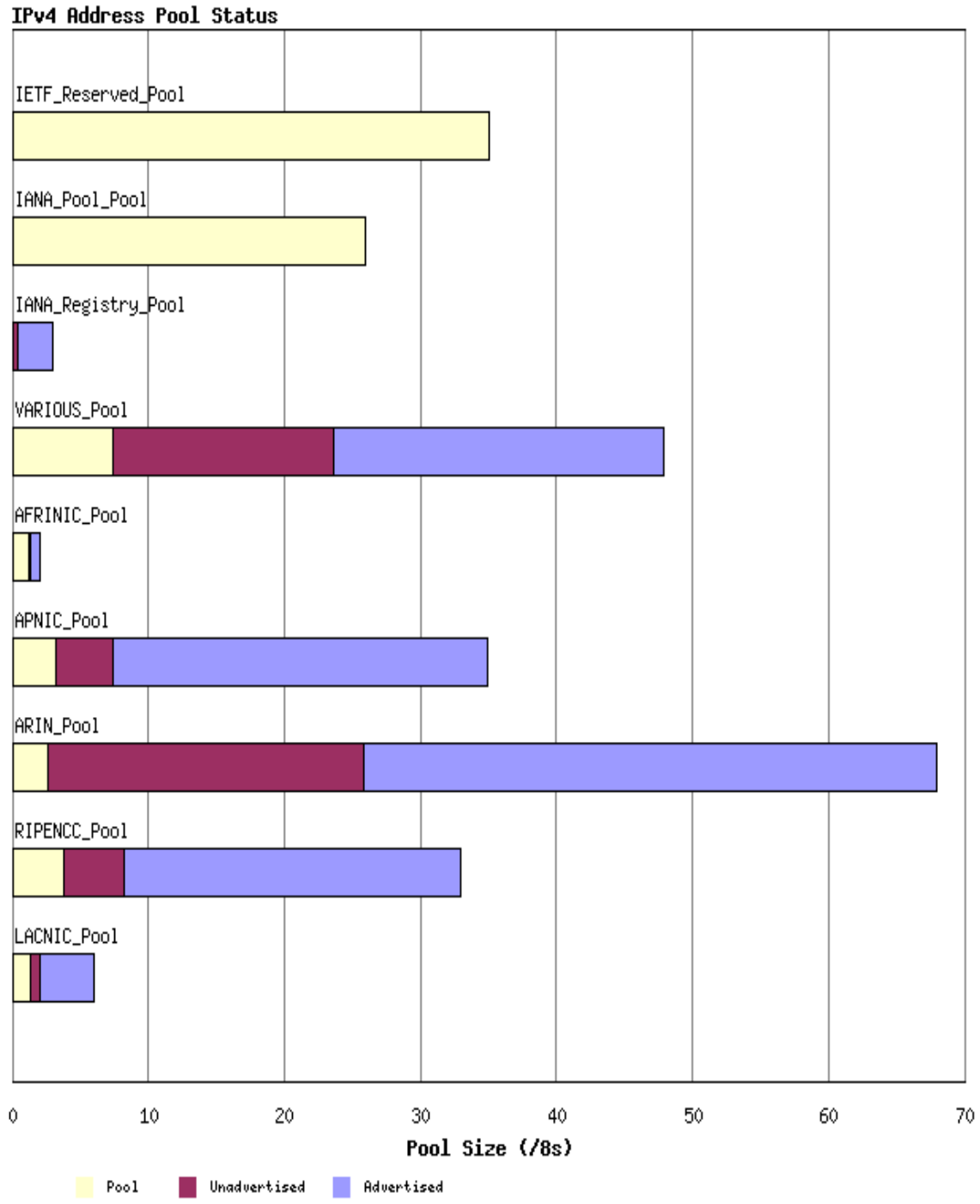


FIGURA 2.12 Estado por RIR
FUENTE: http://www.potaroo.net/tools/ipv4

2.2.5 ESTADO DE LAS DIRECCIONES IPv4.

Una dirección IPv4 puede estar en uno de los 5 estados:

1.- Reservada para uso especial.
Porcentaje - 35.0782

2.- Parte del pool de direcciones no distribuidas por IANA.
Porcentaje - 26

3.- Parte del pool aún no asignado por los RIR.
Porcentaje – 19.3552

4.- Asignada pero no anunciada en los sistemas de enrutamiento.
Porcentaje – 49.1255

5.- Asignada y anunciada en BGP1.
Porcentaje – 126.441

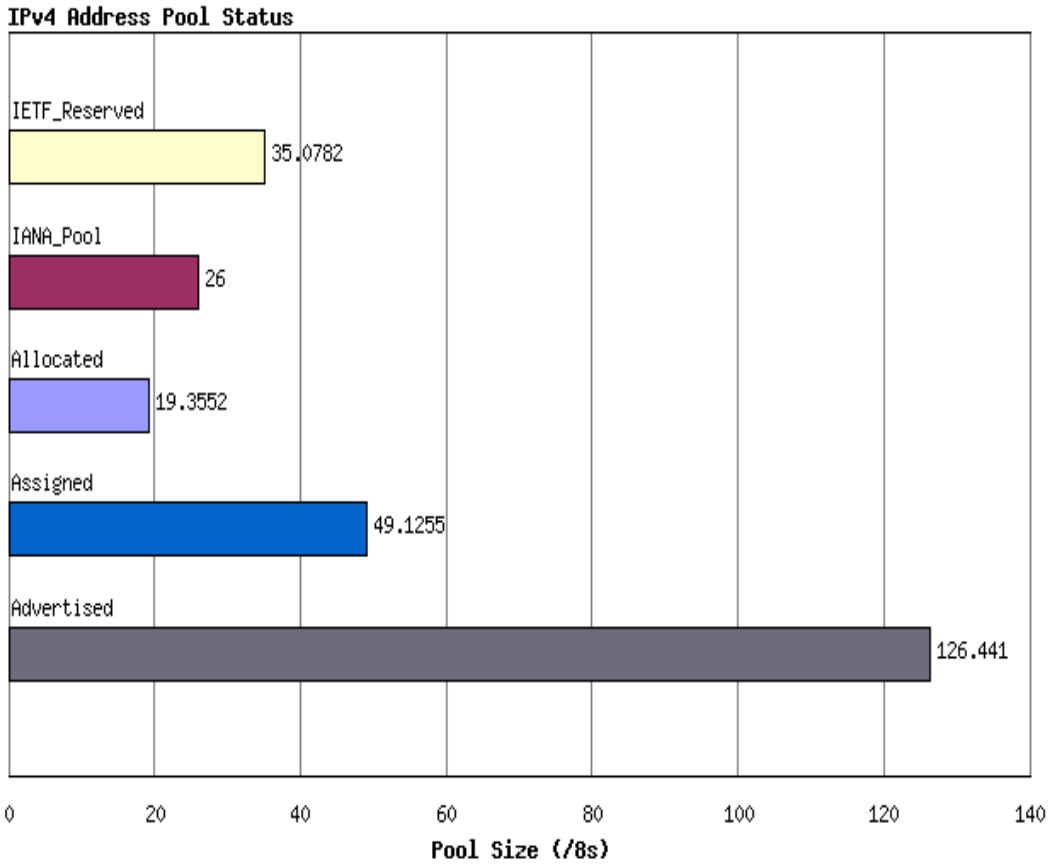


FIGURA 2.13 Estado del Pool de Direcciones
FUENTE: http://www.potaroo.net/tools/ipv4

2.3 PREDICCIONES DE AGOTAMIENTO DEL ESPACIO DE DIRECCIONES IPv4.

Internet está llegando hacia el agotamiento de las direcciones IPv4, es decir, a la progresiva disminución de la cantidad de direcciones IPv4 disponibles. Este tema ha sido una preocupación desde los años 80. Como consecuencia, se ha convertido en el factor impulsor en la creación y adopción de diversas nuevas tecnologías, como CIDR e IPv6; del mismo modo, ha sido un elemento clave en la adopción de NAT.

Cuando IPv4 se diseñó a principios de la década de los 80 su número máximo, pero ideal de direcciones (cuatro mil millones), parecía astronómico, para el 2009 cerca del 81% del total ya han sido asignadas, es decir, sólo queda el 19% del espacio. En cambio, con IPv6 (340 trillones de trillones), no sólo cada habitante del planeta podrá tener su propia dirección, sino que cada célula del cuerpo podría tener una.

Geoff Huston de APNIC predice mediante simulaciones detalladas el agotamiento de la reserva no asignada de IANA para febrero de 2011.Ver Figura 2.14.

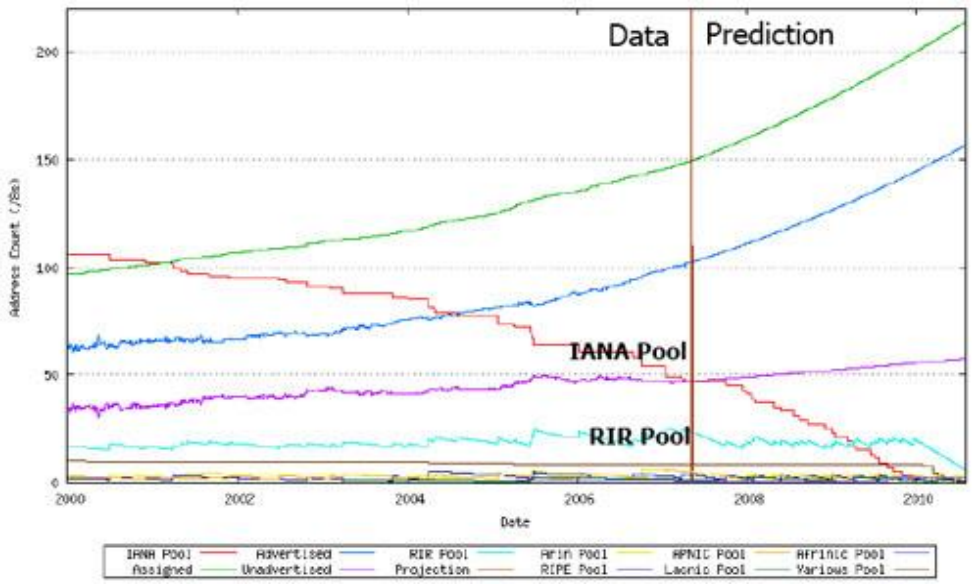


FIGURA 2.14 Estimación según Geoff Huston
FUENTE: http://www.potaroo.net/tools/ipv4

IETF ha previsto que las direcciones IPv4 serán agotadas aproximadamente entre los años 2005 y 2011.

El Registro Americano de Números para Internet (ARIN), el RIR norteamericano, ha pronosticado a la comunidad de Internet del agotamiento previsto para el 2013 como fecha límite para adjudicar el último bloque; así es como lo anunció en un comunicado de su página de Internet [7]

Tony Hain, fabricante de equipos de redes Cisco Systems, predice el agotamiento alrededor de julio de 2010.

El Registro Latino-Americano y Caribeño de Direcciones de Internet (LACNIC), el RIR latinoamericana, sugiere preparar las redes regionales para IPv6 hasta 1 de enero de 2011, por el agotamiento de direcciones IPv4.

2.4 IPv6 (PROTOCOLO DE INTERNET VERSIÓN 6)

Es el más reciente desarrollo del protocolo IP; cuyas especificaciones han sido diseñadas por la Fuerza de Tareas de Ingeniería para Internet (IETF)[8]. El protocolo IP es el mecanismo fundamental que se utiliza para desarrollar las comunicaciones en Internet.

IPv6 es consecuente con las tecnologías desarrolladas en base al protocolo IPv4, de modo tal que incorpora dichas facilidades, y direcciona efectivamente las limitaciones nativas del protocolo IPv4.

De esta manera posibilita e impulsa, la construcción de los nuevos servicios y aplicaciones necesarias para satisfacer las demandas presentes y futuras de las redes TCP/IP avanzadas y de Internet.

---

7. http://www.enterate.unam.mx/Articulos/2007/junio/art1.html

8. Organización de técnicos que administran tareas de ingeniería de telecomunicaciones principalmente de Internet (ejm: mejora de protocolos o darlos de baja, etc.)

IPv6 tiene un espacio de direcciones mucho más grande que IPv4. Esto es consecuencia de la utilización de una dirección de 128 bits, mientras que IPv4 sólo utiliza 32 bits. El nuevo espacio de direcciones por lo tanto, soporta 2^{128} (alrededor de $3,4 \times 10^{38}$) direcciones. Esta expansión proporciona flexibilidad en la asignación de direcciones y el enrutamiento del tráfico y elimina la necesidad primordial de traducción de direcciones de red (NAT), que obtuvo un amplio despliegue como un esfuerzo para aliviar el agotamiento de direcciones IPv4.

2.4.1 MOTIVOS DE UN NUEVO PROTOCOLO

El motivo básico para crear un nuevo protocolo fue la falta de direcciones, IPv4 tiene un espacio de direcciones de 32 bits, en cambio IPv6 ofrece un espacio de 128 bits. El reducido espacio de direcciones de IPv4, junto al hecho de falta de coordinación para su asignación durante la década de los 80, sin ningún tipo de optimización, dejando incluso espacios de direcciones discontinuos, generan en la actualidad, dificultades no previstas en aquel momento.

Otros de los problemas de IPv4 es la gran dimensión de las tablas de ruteo en el backbone de Internet, que lo hace ineficaz y perjudica los tiempos de respuesta.

Debido a la multitud de nuevas aplicaciones en las que IPv4 es utilizado, ha sido necesario agregar nuevas funcionalidades al protocolo básico, aspectos que no fueron contemplados en el análisis inicial de IPv4, lo que genera complicaciones en su escalabilidad para nuevos requerimientos y en el uso simultáneo de dos o más de dichas funcionalidades. Entre las más conocidas se pueden mencionar medidas para permitir la Calidad de Servicio (QoS), Seguridad (IPsec) y movilidad.

2.4.2 LA CABECERA IPv6

La cabecera de un paquete IPv6 es, sorprendentemente, más sencilla que la del paquete IPv4. Y recordemos que además la funcionalidad del protocolo IPv6 es mucho mayor.

La cabecera de un paquete IPv4 es variable, por lo que necesita un campo de tamaño o lenght. Sin embargo, para simplificar la vida de los routers, IPv6 utiliza un tamaño de cabecera fijo de 40 bytes, que componen un total de ocho campos como se muestra en la Figura 2.15: Versión, Clase de Tráfico Etiqueta de Flujo, Tamaño de carga útil, Siguiente cabecera, Límite de saltos, Dirección de Origen, Dirección de Destino

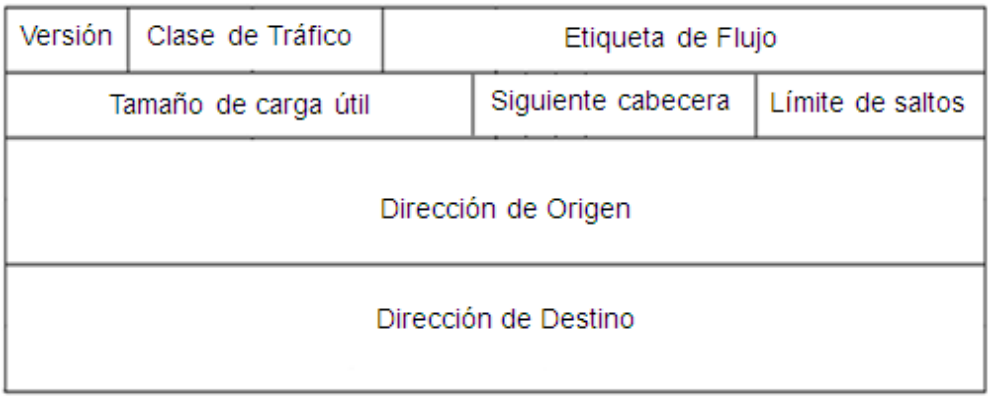


FIGURA 2.15 Encabezado fijo de IPv6

- Versión (4 bits), sirve para que el router se entere de que es un paquete IPv6.

- Dirección origen y de destino (128 bits cada una), son las direcciones de los nodos IPv6 que realizan la comunicación.

- Clase de tráfico (8 bits), para poder diferenciar entre servicios sensibles a la latencia, como VoIP, de otros que no necesitan prioridad, como tráfico http.

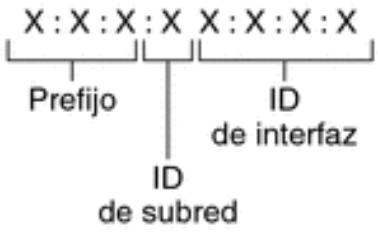
- Etiqueta de flujo (20 bits), permite la diferenciación de flujos de tráfico. Esto tiene importancia a la hora de manejar la calidad de servicio (QoS).

- Siguiente cabecera (8 bits), este campo permite a routers y hosts examinar con más detalle el paquete. A pesar de que el paquete básico IPv6 tiene cabecera de tamaño fijo, el protocolo puede añadir más para utilizar otras características como encriptación y autenticación.

- Tamaño de payload - carga (16 bits), describe el tamaño en octetos de la sección de datos del paquete. Al ser este campo de 16 bits, se podrá usar paquetes de hasta más de 64000 bytes.

2.4.3 PARTES DE UNA DIRECCIÓN IPv6

Una dirección IPv6 tiene un tamaño de 128 bits y se compone de ocho campos de 16 bits, cada uno de ellos unido por dos puntos. Cada campo debe contener un número hexadecimal, a diferencia de la notación decimal con puntos de las direcciones IPv4. En la Figura 2.16, las equis representan números hexadecimales. Donde cada x es el valor hexadecimal.



Ejemplo:

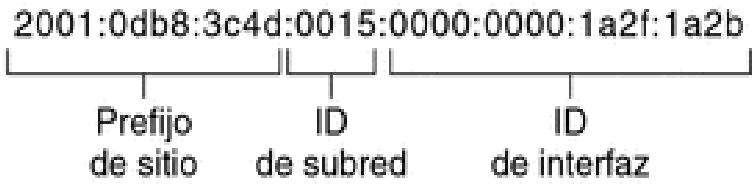


FIGURA 2.16 Formato de direcciones IPv6

Los tres campos que están más a la izquierda (48 bits) contienen el *prefijo de sitio*. El prefijo describe la topología pública que el ISP o el RIR (Regional Internet Registry, Registro Regional de Internet) suelen asignar al sitio.

El campo siguiente lo ocupa el *ID de subred* de 16 bits que el administrador asigna al sitio. El ID de subred describe la topología privada, denominada también topología del sitio, porque es interna del sitio.

Los cuatro campos situados más a la derecha (64 bits) contienen el *ID de interfaz***,** también denominado token**.** El ID de interfaz se configura automáticamente desde la dirección MAC de interfaz o manualmente en formato EUI-64.

Al examinar nuevamente la dirección de la Figura 2.16 (Formato de direcciones IPv6): 2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b se observa que en este ejemplo se muestran los 128 bits completos de una dirección IPv6. Los primeros 48 bits, 2001:0db8:3c4d, contienen el prefijo de sitio y representan la topología pública. Los siguientes 16 bits, 0015, contienen el ID de subred y representan la topología privada del sitio. Los 64 bits que están más a la derecha, 0000:0000:1a2f:1a2b, contienen el ID de interfaz.

2.5 CARACTERÍSTICAS PRINCIPALES DE IPV6

IPv6 fue diseñado como una evolución natural a IPv4. Es decir, todo lo que funcionaba perfectamente en IPv4 se ha mantenido, lo que no funcionaba se ha eliminado, y se ha tratado de añadir nuevas funciones manteniendo la compatibilidad entre ambos protocolos. Las características principales de IPv6 son:

- Mayor espacio de direcciones. El tamaño de las direcciones IP cambia de 32 bits a 128 bits, para soportar más niveles de jerarquías de direccionamiento y más nodos direccionables.

- Optimización del direccionamiento multicast y aparición de anycast.

- Simplificación del formato del “Header”, eliminando algunos campos del Header IPv4 o haciéndolos opcionales.

- Paquetes IP eficientes y extensibles, sin que haya fragmentación en los routers alineados a 64 bits y con una cabecera de longitud fija, más simple, que agiliza su procesado por parte del router.

- Posibilidad de paquetes con carga útil de datos de más de 65.355 bytes.

- Seguridad en el núcleo del protocolo (IPsec).

- Capacidad de etiquetas de flujo. Esta capacidad puede ser usada por un nodo origen para etiquetar paquetes pertenecientes a un flujo (flow) de tráfico particular que requiere manejo especial por los routers IPv6, tal como calidad de servicio no por defecto o servicios de tiempo real.

- Autoconfiguración. La autoconfiguración de direcciones es más simple, especialmente en direcciones “Aggregatable Global Unicast”, los 64 bits superiores son separados por un mensaje desde el router (Router Advertisement) y los 64 bits más bajos son separados con la dirección MAC[9], en este caso, el largo del prefijo de la subred es 64, por lo que no hay que preocuparse por la máscara de red. Además el largo del prefijo no depende del número de los “hosts” por lo tanto, la asignación es más simple.

- Renumeración y "multihoming"[10]. Es posible cambiar el formato de numeración manteniendo la misma dirección IP facilitando así el cambio de proveedor de servicios.

- Direccionamiento más eficiente en el “backbone”[11] de la red, debido a la jerarquía de direccionamiento basada en “aggregation”.

- Mejor calidad de servicio (QoS), clase de servicio (CoS) y capacidad de autenticación y privacidad.

Las características vistas anteriormente son las básicas, ya que la propia estructura del protocolo permite que este crezca o dicho de otro modo, sea escalado, según las nuevas necesidades y aplicaciones o servicios que lo vayan precisando.

---

9. Es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una Ethernet de red.

10. Es una técnica para aumentar la confiabilidad del Conexión del Internet para IP red.

11. Está compuesta de un gran número de routers como son comerciales, gubernamentales, universitarios y otros de gran capacidad interconectados que llevan los datos a través de países, continentes y océanos del mundo mediante mangueras de fibra óptica

2.6 ESPACIO DE DIRECCIONAMIENTO IPv6

Las direcciones IPv6 identifican interfaces de red (ya sea de forma individual o grupos de interfaces). A una misma interfaz de un nodo se le pueden asignar múltiples direcciones IPv6. Dichas direcciones se clasifican en tres tipos:

2.6.1.1 UNICAST

Identificador para una única interfaz. Un paquete enviado a una dirección unicast es entregado sólo a la interfaz identificada con dicha dirección, ver Figura 2.17. Es el equivalente a las direcciones IPv4 actuales.

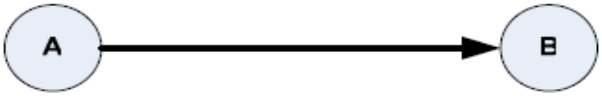


FIGURA 2.17 Direccionamiento Unicast

2.6.1.2 ANYCAST

Identificador para un conjunto de interfaces (típicamente pertenecen a diferentes nodos). Un paquete enviado a una dirección Anycast, es entregado a un miembro cualquiera del grupo, siendo generalmente el más cercano, según la distancia asignada en el protocolo de encaminamiento, como se observa en la Figura 2.18.

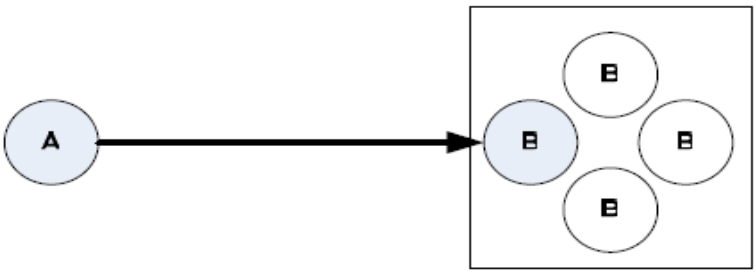


FIGURA 2.18 Direccionamiento Anycast

Permite crear, por ejemplo, ámbitos de redundancia, de forma que varias máquinas puedan ocuparse del mismo tráfico según una secuencia determinada (por el routing), si la primera “cae”. Las direcciones Anycast sólo se pueden utilizar en “routers”.

2.6.1.3 MULTICAST

Identificador para un grupo de interfaces (por lo general pertenecientes a diferentes nodos). Cuando un paquete es enviado a una dirección multicast es entregado a todas las interfaces que se encuentran agrupados bajo dicha dirección. Observe Figura 2.19.

En el IPv6 no existen direcciones broadcast, su funcionalidad ha sido mejorada por las direcciones multicast.

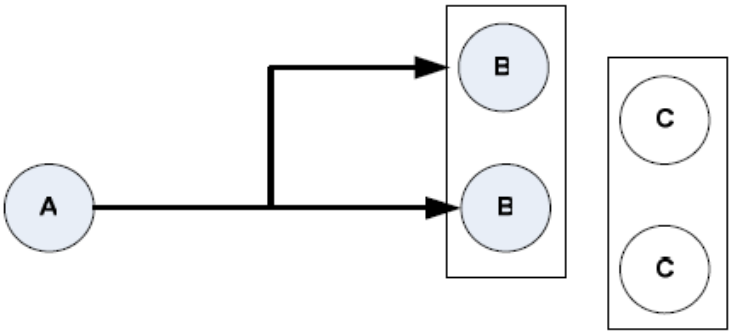


FIGURA 2.19 Direccionamiento Multicast

2.6.2 IDENTIFICACIÓN DE LOS TIPOS DE DIRECCIONES

Los tipos de direcciones IPv6 pueden identificarse tomando en cuenta los primeros bits de cada dirección.

:: /128. Dirección indefinida. Todo ceros, máscara de 128 bits se utiliza para indicar la ausencia de dirección, y no se asigna a ningún nodo.

::1 /128 Dirección de loopback es una dirección que puede usar un nodo para enviarse paquetes a sí mismo (corresponde con 127.0.0.01 de IPv4). No puede asignarse a ninguna interfaz física.

:: /96 (La máscara cubre toda la dirección excepto los últimos 4 bytes) Dirección IPv4 compatible se usa como un mecanismo de transición en las redes duales IPv4/IPv6. Es un mecanismo obsoleto.

::1.2.3.4 La dirección IPv4 compatible se usa como un mecanismo de transición en las redes duales IPv4/IPv6. Mecanismo que no se usa.

::ffff:0:0 /96 Dirección IPv4 mapeada es usada como un mecanismo de transición en redes duales.

fe80:: /10 Prefijo de enlace local (en inglés *link local*) específica que la dirección sólo es válida en el enlace físico local.

fec0:: /10 Prefijo de emplazamiento local (site-local prefix) específica que la dirección sólo es válida dentro de una organización local. Se deben sustituir por direcciones Local IPv6 Unicast.

ff00:: /8 Prefijo de difusión (multicast). Usada para direcciones multicast.

ff01::1 Funcionalidad de todos los nodos (broadcast) utilizando difusión (multicast).

2.7 LA AUTOCONFIGURACIÓN EN IPv6

Es el conjunto de pasos por los cuales un host decide como auto configurar sus interfaces en Ipv6. Este mecanismo es el que nos permite afirmar que IPv6 es "Plug & Play"[12]

El proceso incluye la creación de una dirección de enlace local, verificación de que no está duplicada en dicho enlace y determinación de la información que ha de ser auto configurada (direcciones y otra información). Las direcciones pueden obtenerse de forma totalmente manual, mediante DHCPv6 (statefull o configuración predeterminada), o de forma automática (stateless o descubrimiento automático, sin intervención).

12. Enchufar y usar. Se refiere a la capacidad de un sistema informático de configurar automáticamente los dispositivos al conectarlos

2.7.1 TIPOS DE AUTOCONFIGURACIÓN

Existen dos tipos de autoconfiguración y son:

La autoconfiguración **“stateless”** (sin intervención), no requiere ninguna configuración manual del host, configuración mínima (o ninguna) de routers, y no precisa servidores adicionales. Permite a un host generar su propia dirección mediante una combinación de información disponible localmente e información anunciada por los routers.

Los routers anuncian los prefijos que identifican la subred (o subredes) asociadas con el enlace, mientras el host genera un “identificador de interfaz”, que identifica de forma única la interfaz en la subred. La dirección se compone por la combinación de ambos campos. En ausencia de router, el host sólo puede generar la dirección de enlace local, aunque esto es suficiente para permitir la comunicación entre nodos conectados al mismo enlace.

En la autoconfiguración **“stateful”** (predeterminada), el host obtiene la dirección de la interfaz y/o la información y parámetros de configuración desde un servidor. Los servidores mantienen una base de datos con las direcciones que han sido asignadas a cada host.

2.8 ENRUTAMIENTO CON IPv6

El enrutamiento es el proceso de reenviar paquetes entre segmentos de red conectados. En las redes basadas en IPv6, el enrutamiento es la parte de IPv6 que proporciona capacidades de reenvío entre hosts que se encuentran en segmentos independientes que pertenecen a una red mayor basada en IPv6.

Una de las ventajas de IPv6 es el mecanismo de enrutamiento flexible. Debido a la forma en que los Id de red de IPv4 se asignaban y se asignan, los principales enrutadores de Internet deben mantener grandes tablas de enrutamiento.

Estos enrutadores deben conocer todas las rutas para poder reenviar los paquetes que se dirigen potencialmente a cualquier nodo de Internet. Con su capacidad de agregar direcciones, IPv6 permite direcciones flexibles y reduce drásticamente el tamaño de las tablas de enrutamiento. En esta nueva arquitectura de direccionamiento, los enrutadores intermedios sólo deben mantener el seguimiento de la parte local de su red para reenviar los mensajes de forma adecuada.

2.8.1 ENRUTADORES IPv6

Los segmentos de red IPv6, denominados también vínculos o subredes, están conectados mediante enrutadores IPv6, que son dispositivos que pasan paquetes IPv6 de un segmento de red a otro. Este proceso se conoce como enrutamiento IPv6 y se muestra en la Figura 2.20.

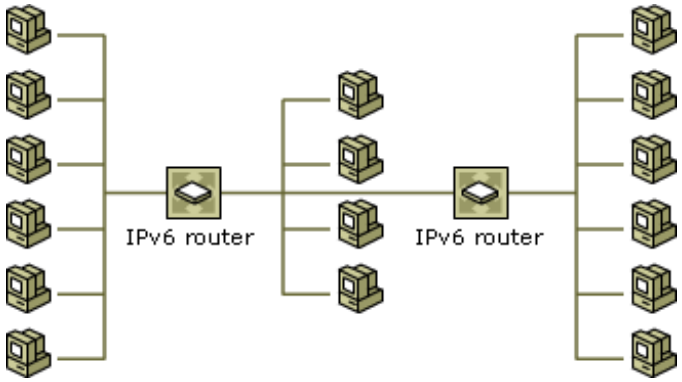


FIGURA 2.20 Enrutamiento IPv6

Los enrutadores IPv6 proporcionan el medio principal para unir dos o más segmentos de red IPv6 físicamente independientes. Todos los enrutadores IPv6 tienen las características siguientes:

- Los enrutadores IPv6 son físicamente hosts múltiples. Un host de hosts múltiples físicos es un host de la red que utiliza dos o más interfaces de conexión de red para conectarse a cada segmento de red físicamente independiente.

- Los enrutadores IPv6 permiten el reenvío de paquetes a otros hosts IPv6. Los enrutadores IPv6 son diferentes de otros hosts que utilizan la característica de multitarjeta. Un enrutador IPv6 debe ser capaz de reenviar la comunicación basada en IPv6 entre redes para otros hosts de la red IPv6.

Los enrutadores IPv6 se pueden implementar mediante diversos productos de hardware y software, comúnmente se utilizan enrutadores que son dispositivos de hardware dedicados que ejecutan software especializado, independientemente del tipo de enrutadores IPv6 que se utilicen, todo el enrutamiento IPv6 depende del uso de una tabla de enrutamiento para la comunicación entre los segmentos de red.

2.8.2 TABLAS DE ENRUTAMIENTO

Los hosts IPv6 utilizan una tabla de enrutamiento para mantener información acerca de otras redes y hosts IPv6. Los segmentos de red se identifican mediante un prefijo de red IPv6 y una longitud de prefijo. Además, las tablas de enrutamiento proporcionan información importante a cada host local respecto a cómo deben comunicarse con redes y hosts remotos.

En cada equipo de una red IPv6, se puede mantener una tabla de enrutamiento con una entrada para cada equipo o red que se comunique con el equipo local, en general, esto no es práctico y, en su lugar, se utiliza un enrutador predeterminado.

Antes de enviar un paquete IPv6, el equipo inserta la dirección IPv6 de origen y de destino (para el destinatario) en el encabezado IPv6. A continuación, el equipo examina la dirección IPv6 de destino, la compara con una tabla de enrutamiento IPv6 mantenida localmente y realiza la acción adecuada.

El equipo realiza una de las tres acciones siguientes:

- Pasa el paquete a un nivel de protocolo superior a IPv6 en el host local.
- Reenvía el paquete a través de una de las interfaces de red conectadas.
- Descarta el paquete.

IPv6 busca en la tabla de enrutamiento la ruta más similar a la dirección IPv6 de destino. La ruta, en orden de más a menos específica, se determina de la manera siguiente:

- Una ruta que coincide con la dirección IPv6 de destino (una ruta de host con una longitud de prefijo de 128 bits).
- Una ruta que corresponde al destino con la mayor longitud de prefijo.
- La ruta predeterminada (el prefijo de red ::/0).

2.9 PROCESO DE SOLICITUD DE DIRECCIONES IPv6

Esquema de administración de los recursos de Internet es jerárquico y sigue el siguiente esquema:

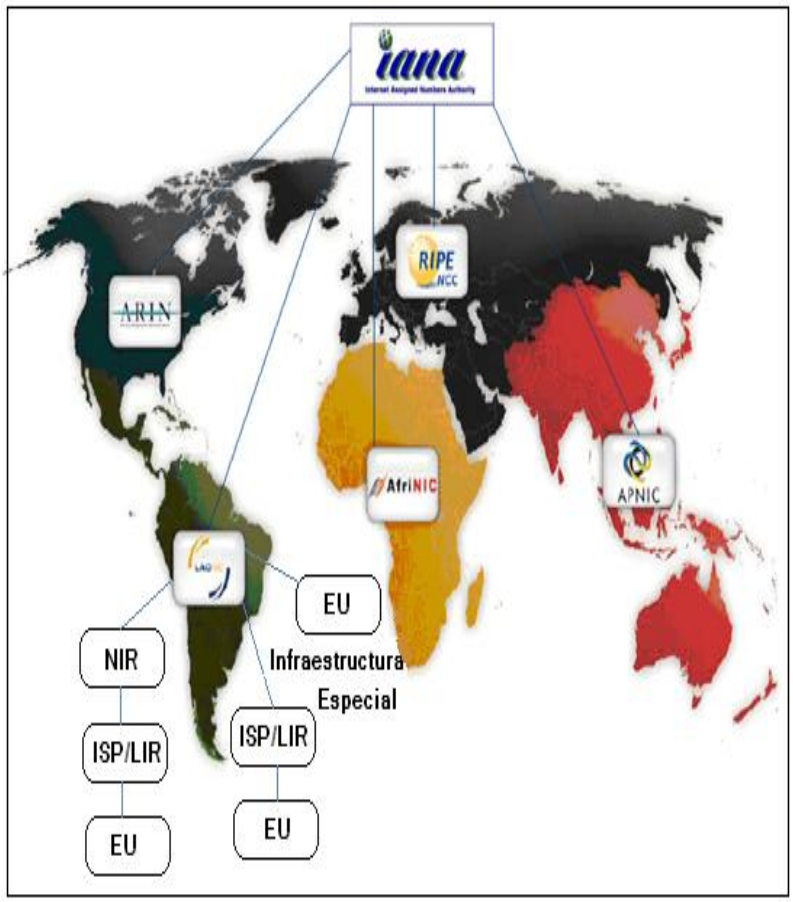


FIGURA 2.21 Registros de Internet Regionales
FUENTE: http://www.iana.org/

2.9.1 IANA (INTERNET ASSIGNED NUMBER AUTHORITY)

IANA es responsable de distribuir parte del espacio global de las direcciones IP y los números de sistemas autónomos a Registros Regionales de acuerdo a necesidades establecidas.

2.9.2 REGISTRO DE INTERNET REGIONAL (RIR)

Los registros de Internet Regionales (RIRs) son establecidos y autorizados por las comunidades regionales respectivas, y reconocidos por el IANA para servir y representar grandes regiones geográficas.

Los RIRs organizaciones sin fines de lucro que adjudican o confieren direcciones IP a proveedores de Internet, en Norteamérica y Latinoamérica respectivamente.

Estos obtienen los bloques de direcciones de la IANA, la jerarquía de adjudicaciones y asignaciones de los recursos de Internet se muestran en la Figura 2.21.

Hay actualmente 5 RIRs en funcionamiento:

- **ARIN** (American Registry for Internet Numbers).
  Para América del Norte.
- **RIPE NCC** (Network Coordination Centre).
  Para Europa, el Oriente Medio y Asia Central.
- **APNIC** (Asia-Pacific Network Information Centre).
  Para Asia y la Región Pacífica.
- **LACNIC** (Latin American and Caribbean Internet Address Registry).
  Para América Latina y el Caribe.
- **AFRINIC** (African Network Information Centre).
  Para África.

Para el área de Latinoamérica y el Caribe el espacio de direcciones IP es distribuido por IANA a LACNIC para ser a su vez distribuidos y asignados a Registros Nacionales de Internet (NIR), Proveedores de Servicios de Internet (ISP) y usuarios finales.

2.9.3 LACNIC (REGISTRO DE DIRECCIONES DE INTERNET PARA AMÉRICA LATINA Y EL CARIBE)

Es la organización responsable de la asignación y administración de las Direcciones IP para la región de América Latina y el Caribe, siendo uno de los 5 Registros Regionales de Internet en el mundo.

2.9.4 REGISTRO DE INTERNET (IR)

Es una organización responsable de la distribución de espacios de direcciones IP a sus miembros o clientes y del registro de esa distribución.

2.9.5 REGISTRO DE INTERNET NACIONAL (NIR)

Un NIR distribuye, principalmente, los recursos de Internet a sus miembros o constituyentes, los cuales generalmente son LIRs.

2.9.6 REGISTRO DE INTERNET LOCAL (LIR)

Un LIR es un IR que a su vez asigna recursos de Internet a usuarios de los servicios de red que éste provee. Los LIRs son generalmente ISPs, cuyos clientes son principalmente usuarios finales y posiblemente otros ISPs.

2.9.7 PROVEEDOR DE SERVICIOS DE INTERNET (ISP)

Asigna principalmente espacio de direcciones IP a los usuarios finales de los servicios de red que éste provee. Sus clientes pueden ser otros ISPs. Los ISPs no tienen restricciones geográficas como lo tienen los NIRs.

2.9.8 SITIO FINAL O USUARIO FINAL (EU)

Un usuario final es aquel que tiene una relación de negocios con un proveedor de servicios Internet que involucra:

- Al proveedor asignando un espacio de direcciones al usuario final.
- Al proveedor otorgando un servicio de tránsito para el usuario final hacia otros sitios.
- Al proveedor de servicios transportando el tráfico del usuario final.
- Al proveedor anunciando un prefijo de ruta agregado que contiene el rango asignado por LACNIC al usuario final.

CAPÍTULO 3.

BGP (BORDER GATEWAY PROTOCOL)

El BGP o Border Gateway Protocol, es un protocolo mediante el cual se intercambian información de encaminamiento entre sistemas autónomos a la vez que garantiza una elección de rutas libres de bucles.

Es el protocolo principal de publicación de rutas utilizado por las compañías más importantes de ISP en Internet.

En este capítulo, se hablará todo lo referente a BGP conceptos básicos, iBGP y eBGP, atributos de ruta de acceso, selección de rutas, BGP con IPv6 entre otros temas relacionados.

3.1 FUNCIONES DE LA CAPA DE RED DEL MODELO OSI

Capa de Red o Capa Internet: Es la encargada de enviar los datos a través de las distintas redes físicas que pueden conectar una máquina origen con la de destino de la información.

Las funciones desempeñadas en la capa de red del modelo OSI se enumeran a continuación:

- Tráfico a la dirección de destino final.
- Abordar; lógico direcciones de red y servicios de direcciones.
- Funciones de enrutamiento, la ruta de descubrimiento y la selección de rutas.
- Conmutación de paquetes.
- Secuencia de paquetes de control.
- De extremo a extremo la detección de errores, a partir de los datos del remitente al receptor de los datos.
- Control de la congestión.
- Capa de red, control de flujo y la capa de control de errores de red.
- Portal de servicios.

3.2 IGP y EGP, PROTOCOLOS ENRUTADOS Y PROTOCOLOS DE ENRUTAMIENTO

3.2.1 PROTOCOLO ENRUTADO

Se usa para dirigir el tráfico generado por los usuarios, proporcionando información suficiente en su dirección de la capa de red, para permitir que un paquete pueda ser enviado desde un host a otro, basado en el esquema de direcciones.

Ejemplos de protocolos enrutados:

- Protocolo Internet (IP)[13].
- Intercambio de paquetes de internetwork (IPX)[14].

1.1.1 PROTOCOLO DE ENRUTAMIENTO

Manejan la información de rutas para el envío de paquetes entre routers. Un protocolo de enrutamiento permite que un router comparta información con otros routers, acerca de las redes que conoce así como de su proximidad a otros routers.

La información que un router obtiene de otro, mediante el protocolo de enrutamiento, es usada para crear y mantener las tablas de enrutamiento.
Ejemplos de protocolos de enrutamiento:

- Protocolo de información de enrutamiento (RIP).
- Protocolo de enrutamiento de gateway interior (IGRP).
- Protocolo de enrutamiento de gateway interior mejorado (EIGRP).
- Protocolo "Primero la ruta más corta" (OSPF), los cuáles se detallarán más adelante.

---

13 Es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados.

14 Es un protocolo de datagramas rápido orientado a comunicaciones sin conexión que se encarga de transmitir datos a través de la red, incluyendo en cada paquete la dirección de destino.

3.2.2.1 PROTOCOLO DE PASARELA INTERNO (IGP, INTERIOR GATEWAY PROTOCOL)

Se usan para el enrutamiento dentro de sistemas autónomos.

SISTEMA AUTÓNOMO (AS)

Es un conjunto de redes bajo una administración común, las cuales comparten una estrategia de enrutamiento común. Para el mundo exterior, el AS es una entidad única, este puede ser administrado por uno o más operadores, a la vez que presenta un esquema unificado de enrutamiento hacia el mundo exterior.

Los números de identificación de cada AS son asignados por el Registro estadounidense de números de la Internet (ARIN), tema que se vio en el Capítulo 2, los proveedores de servicios o el administrador de la red. Este sistema autónomo es un número de 16 bits. Los protocolos de enrutamiento tales como el IGRP de Cisco, requieren un número único de sistema autónomo.

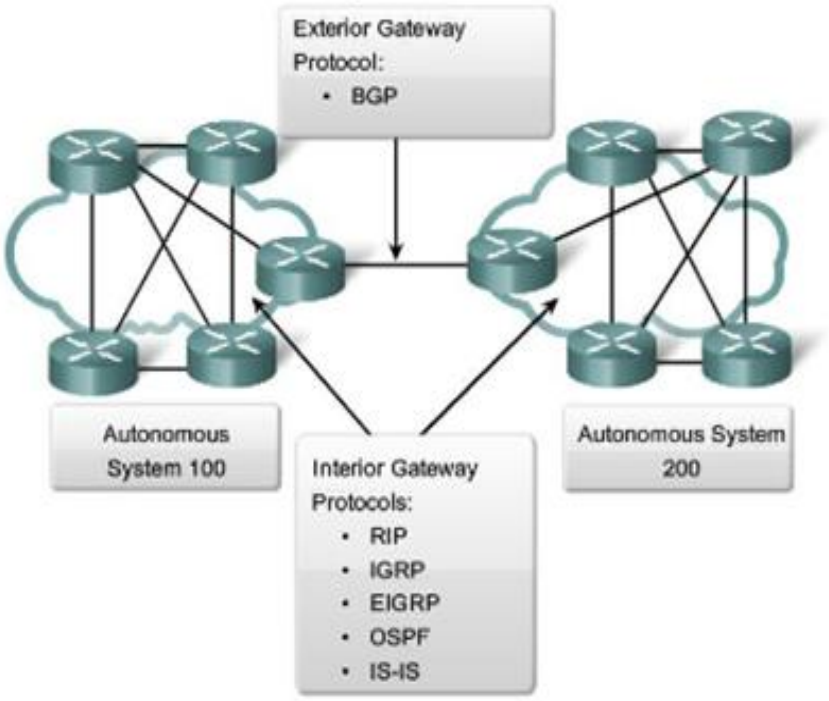


FIGURA 3.22 Conexión entre Sistemas Autónomos
FUENTE: http://www.cisco.com

Los protocolos de pasarela interior se pueden dividir en dos categorías:

3.2.2.1.1 PROTOCOLOS DE VECTOR DISTANCIA

El enrutamiento por vector-distancia determina la dirección y la distancia (vector) hacia cualquier enlace en la internetwork. La distancia puede ser el número de saltos hasta el enlace. Los enrutadores que utilizan los algoritmos de vector-distancia envían todos o parte de las entradas de su tabla de enrutamiento a los enrutadores adyacentes de forma periódica.

Este conjunto de protocolos tienen el inconveniente de ser algo lentos, si bien es cierto que son sencillos de manejar y muy adecuados para redes compuestas por pocas máquinas. Ejemplos de este tipo de protocolos son:

3.2.2.1.1.1 PROTOCOLO DE INFORMACIÓN DE ENRUTAMIENTO (RIP, ROUTING INFORMATION PROTOCOL)

Es un protocolo universal de enrutamiento por vector de distancia que utiliza el número de saltos como único sistema métrico. Un salto es el paso de los paquetes de una red a otra. Si existen dos rutas posibles para alcanzar el mismo destino, RIP elegirá la ruta que presente un menor número de saltos.

El RIP permite que los routers determinen cuál es la ruta que se debe usar para enviar los datos. Utiliza el protocolo UDP y se comunica a través del puerto 520. Tiene la ventaja de ser muy fácil de configurar.

- Es un protocolo de enrutamiento por vector distancia.
- La única medida que utiliza (métrica) es el número de saltos.
- El número máximo de saltos es de 15.
- Se actualiza cada 30 segundos.
- No garantiza que la ruta elegida sea la más rápida.
- Genera mucho tráfico con las actualizaciones de sus tablas.

3.2.2.1.1.2 PROTOCOLO DE ENRUTAMIENTO DE GATEWAY INTERIOR (IGRP, INTERIOR GATEWAY ROUTING PROTOCOL)

IGRP fue diseñado por Cisco a mediados de los ochenta, para corregir algunos de los defectos de RIP y para proporcionar un mejor soporte para redes grandes con enlaces de diferentes anchos de banda, siendo un protocolo propietario de Cisco.

3.2.2.1.1.3 PROTOCOLO DE ENRUTAMIENTO DE PASARELA INTERIOR (EIGRP; E=ENHANCED)

Basado en IGRP y como mejora de este, es un protocolo híbrido que pretende ofrecer las ventajas de los protocolos por vector de distancia y las ventajas de los protocolos de estado de enlace. Utiliza el protocolo TCP/IP y determina la ruta basándose en el ancho de banda, el retardo, la fiabilidad y la carga del enlace.

3.2.2.1.3 PROTOCOLOS ESTADO DE ENLACE (LINK STATE)

Utiliza un modelo de base de datos distribuida y replicada. Los routers intercambian paquetes de estado de enlace que informa a todos los routers de la red sobre el estado de sus distintos interfaces.

Esto significa que sólo se envía información acerca de las conexiones directas de un determinado router, y no toda la tabla de enrutamiento como ocurre en el enrutamiento por vector de distancia.

Los protocolos de estado de enlace no pueden proporcionar una solución de conectividad global, como la que se requiere en grandes redes como Internet, pero si son utilizados por muchos proveedores como protocolo de enrutamiento en el interior de un SA.

Los protocolos más conocidos son OSPF e IS-IS. Algunos de los beneficios de estos protocolos son:

- No hay límite en el número de saltos de una ruta. Los protocolos del estado de enlace trabajan sobre la base de las métricas de enlace en lugar de hacerlo en función del número de saltos.

- El ancho de banda del enlace y los retrasos puede ser factorizados cuando se calcule la ruta más corta hacia un destino determinado.

- Los cambios de enlace y nodo son inmediatamente introducidos en el dominio mediante actualizaciones del estado de enlace.

- Soporte para VLSM y CIDR, ya que intercambian información de máscara en las actualizaciones.

3.2.2.1.2.1 PRIMERO LA RUTA LIBRE MÁS CORTA (OSPF, OPEN SHORTEST PATH FIRST)

Es un protocolo universal basado en el algoritmo de estado de enlace, desarrollado por el IETF para sustituir a RIP. Básicamente, utiliza un algoritmo que le permite calcular la distancia más corta entre la fuente y el destino al determinar la ruta para un grupo específico de paquetes. OSPF es uno de los protocolos del estado de enlace más importantes, basado en las normas de código abierto, lo que significa que muchos fabricantes lo pueden desarrollar y mejorar.

3.2.2.1.2.2 SISTEMA INTERMEDIO A SISTEMA INTERMEDIO (IS-IS, INTERMEDIATE SYSTEM TO INTERMEDIATE SYSTEM)

Parecido a OSPF en tanto que ambos utilizan el estado de enlace para resolver las rutas, pero IS-IS tiene la ventaja de, por ejemplo, soporte para IPv6, lo que permite conectar redes con protocolos de encaminamiento distinto.

3.2.2.2 PROTOCOLO DE PASARELA EXTERIOR (EGP, EXTERIOR GATEWAY PROTOCOLO)

Se usan para el enrutamiento entre sistemas autónomos.

El ejemplo típico de protocolo de pasarela exterior (EGP) es el BGP (Border Gateway Protocol).

3.3 CRITERIOS DE SELECCIÓN DE PROTOCOLOS DE ENRUTAMIENTO

Todos los protocolos de enrutamiento tienen la misma meta general: compartir información sobre alcanzabilidad entre enrutadores, así mismo todos tienen ventajas y desventajas.

La selección de un protocolo debe basarse en las necesidades de la red para lo cual es útil contrastar las mismas con las características de cada uno descritas en el numeral anterior.

Los aspectos a considerar son:

- Enrutamiento interior al AS o exterior.
- Protocolos dinámicos vs estáticos vs ruta por defecto.
- Las métricas que soportan.
- Protocolos de vector distancia vs estado de enlace.
- Tiempo de convergencia.
- Basados en clases o sin clases (con máscara).
- Escalabilidad.

3.4 BGP (BORDER GATEWAY PROTOCOL)

Es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos.

Por ejemplo, como se muestra en la Figura 3.2, los ISP registrados en Internet suelen componerse de varios sistemas autónomos (en este caso de dos redes OSPF e EIGRP) y para este caso es necesario un protocolo como BGP.

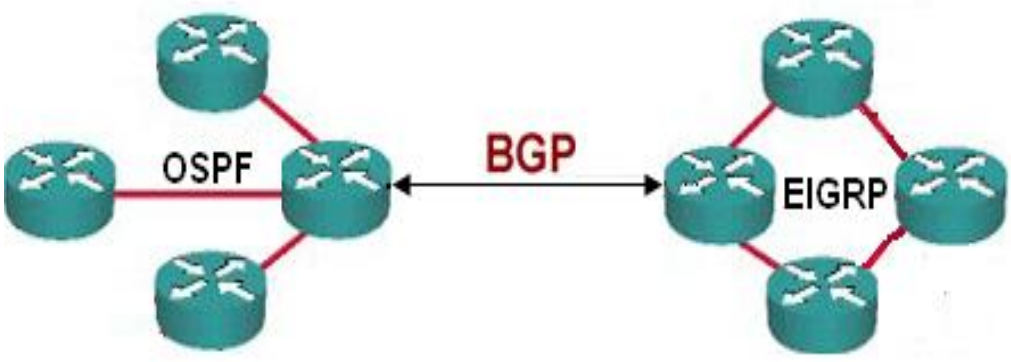


FIGURA 3.23 Conexión de dos redes mediante BGP

BGP, es el sistema que utilizan los grandes nodos de Internet para comunicarse entre ellos y transferir una gran cantidad de información entre dos puntos de la Red. Su misión es encontrar el camino más eficiente entre los nodos para propiciar una correcta circulación de la información en Internet.

BGP es un protocolo muy complejo que se usa en la interconexión de redes conectadas por un backbone de internet. Este protocolo usa parámetros como ancho de banda, precio de la conexión, saturación de la red, denegación de paso de paquetes, etc. Para enviar un paquete por una ruta o por otra.

Un router BGP da a conocer sus direcciones IP a los enrutadores BGP y esta información se difunde por los enrutadores BGP cercanos y no tan cercanos. BGP tiene sus propios mensajes entre enrutadores, no utiliza RIP.

3.4.1 TIPOS DE MENSAJES BGP

BGP utiliza cinco tipos de mensaje para negociar sus parámetros, intercambiar la información de encaminamiento o indicar los errores. Cada mensaje tiene un tamaño de entre 19 y 4096 bytes, y depende del TCP/IP para su entrega, secuenciamiento y fragmentación. Esto implica que los mensajes múltiples BGP se pueden enviar en un segmento TCP. Todos los mensajes incluyen una cabecera común de 19 bytes, y a continuación datos adicionales dependiendo del tipo de mensaje. En los mensajes BGP se suele codificar la información con el formato Tipo-Longitud-Valor (TLV) para proporcionar flexibilidad, extensibilidad y facilidad en el proceso de los mensajes y de sus datos.

3.4.1.1 MENSAJE OPEN – ABRIR (TIPO 1)

El primer mensaje BGP que se envía después de que la conexión TCP se ha establecido es el mensaje OPEN. Este tipo de mensaje se emplea para intercambiar información de configuración y negociar los parámetros comunes de la sesión punto a punto.

3.4.1.2 MENSAJE UPDATE - ACTUALIZACIÓN (TIPO 2)

Los mensajes UPDATE se utilizan para distribuir información de encaminamiento en BGP, y son enviados únicamente con posterioridad al establecimiento de la sesión. Un mensaje UPDATE puede ser usado para eliminar rutas existentes, añadir nuevas rutas o ambas cosas.

3.4.1.3 MENSAJE KEEPALIVE (TIPO 3)

Los mensajes KEEPALIVE son enviados periódicamente para indicar que el enlace punto a punto se encuentra todavía operativo. Se usa para mantener activa la sesión BGP. El mensaje contiene sólo cabecera y ningún tipo de datos.

3.4.1.4 MENSAJE NOTIFICATION - NOTIFICACIÓN (TIPO 4)

El mensaje de NOTIFICATION, se envía cuando el protocolo BGP detecta que se ha producido un error, después del cual se ha cerrado la sesión y la conexión TCP. La causa del error se envía al otro extremo para ser depurada.

3.5 iBGP y eBGP

Aunque BGP es un protocolo de routing exterior, dispone de dos comportamientos o peering:

- Externo - External BGP (eBGP)
- Interno - Internal BGP (iBGP)

En la Figura 3.3 se observa que la diferencia depende de la función del protocolo de routing, es el router el que determinará si él será un vecino eBGP o iBGP comprobando el número de AS en las actualizaciones.

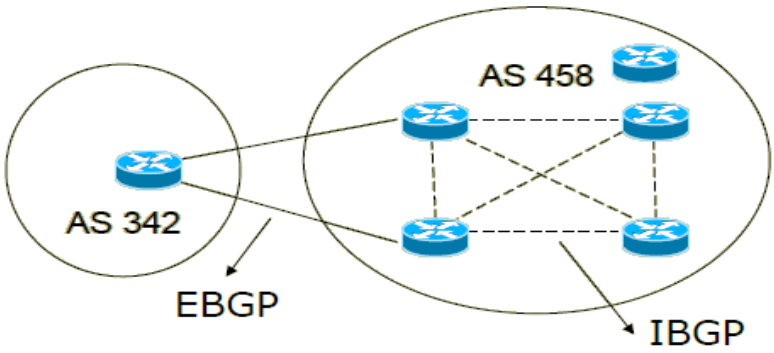


FIGURA 3.24 iBGP vs. eBGP

3.5.1 eBGP

Es el modo “habitual” de utilizar BGP, ya que después de todo BGP se diseño para intercambiar rutas entre diferentes Sistemas Autónomos en Internet. Los enrutadores fronterizos de un AS determinado se conectan a los enrutadores de otros AS a través de sesiones BGP.

Estos enrutadores proporcionan los únicos puntos de entrada y salida de sus AS. Implementan reglas de filtrado de rutas e intercambian un subconjunto de las mismas mediante BGP y enrutadores en otros AS a través de sesiones BGP.

eBGP usados para

- Intercambiar prefijos con otros AS
- Implementar políticas de ruteo

3.5.2 iBGP

Si un AS en concreto tiene varios portavoces BGP y proporciona servicio de tránsito para otros AS (como suele ser el caso, al menos para un número reducido de rutas), debe prestarse atención para garantizar una visibilidad constante de las rutas dentro del AS.

En general, cada AS tendrá más de un enrutador fronterizo que participará en las sesiones eBGP con los AS próximos. Durante este proceso, cada enrutador eBGP obtendrá información sobre algún subconjunto de reglas conocidas por el AS. Como uno de los objetivos del BGP es permitir que cada AS sea tratado como una entidad monolítica abstracta, es fundamental que cada enrutador del AS tenga un concepto completo de las rutas disponibles para el eBGP en todo el AS.

La coherencia se consigue permitiendo que los enrutadores fronterizos intercambien información mediante iBGP. Los enrutadores eBGP se conectan entre sí dentro del AS y mantienen sesiones iBGP entre sí. Estas sesiones permiten que cada enrutador actualice sus tablas con la información contenida en el resto.

Es importante señalar que un iBGP no es un IGP como RIP o OSPF. De hecho, los mensajes enviados durante una sesión iBGP se encaminan dentro del AS con cualquier IGP que esté operativo. Las sesiones iBGP sólo proporcionan un medio por el cual los enrutadores dentro de un AS pueden utilizar el mismo protocolo (BGP) para intercambiar información completa.

iBGP usado para transportar:

- Los prefijos de Internet a través del Backbone.
- Los prefijos de los clientes.
- Usar Peer Groups.
- Usar Passwords en la sesiones de IBGP.

3.6 ATRIBUTOS DE LA RUTA DE ACCESO

Los atributos de ruta BGP son un grupo de parámetros que describen las características de una ruta. El protocolo BGP empareja los atributos con la ruta que describen y, a continuación, compara todas las rutas disponibles para un destino para así seleccionar la mejor ruta de acceso a ese destino.

En el la Figura 3.4, se ilustra la forma general el campo tipo Atributos de ruta de acceso. Banderas del atributo Código de tipo del atributo

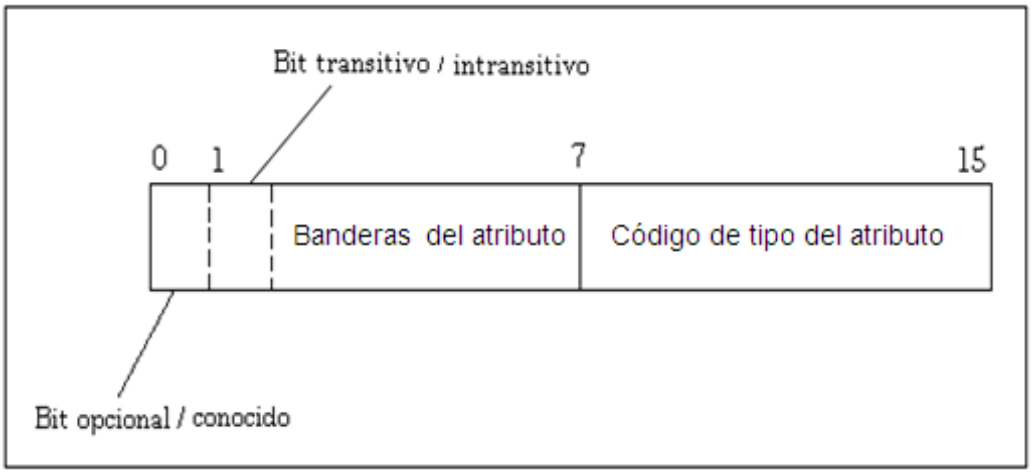


FIGURA 3.4 Formato del tipo de atributo de ruta de acceso

Estas cuatro categorías son descritas por los dos primeros bits de campo *Flags* del atributo:

- El primer bit (0) del campo *Flags* del atributo indica si el atributo es conocido (0) u opcional (1).

- El segundo bit (1) indica si el atributo opcional es intransitivo (0) o transitivo (1). Los atributos conocidos son siempre transitivos, por lo que el segundo bit siempre es uno.

- El tercer bit (2) indica si la información del atributo transitivo opcional es completa (0) o parcial (1).

- El cuarto bit (3) define si la longitud del atributo es de 1 byte (0) o de dos bytes (1).

- Los cuatro bits de menor orden (4 al 7) del campo *Flags* del atributo actualmente no se usan y son siempre 0.

3.6.1 CATEGORÍAS DE LOS ATRIBUTOS EN BGP

Se dividen en dos partes:

- Well-known: Atributos que su utilización es obligatoria.
- Optional: Atributos opcionales.

WELL-KNOWN (Conocido)

- **OBLIGATORIO CONOCIDO.** Estos atributos son requeridos y deben ser reconocidos por todas las implementaciones de BGP.

- **DISCRECIONAL CONOCIDO.** Estos atributos no son requeridos, pero en el caso de estar presentes todos los enrutadores que ejecuten BGP tiene que reconocerlos y actuar en la información que contienen.

OPTIONAL (Opcional)

- **TRANSITIVO OPCIONAL.** El router no debe de reconocer estos atributos, pero si este es el caso, marcará la actualización como parcial y enviará la actualización completa con los atributos, al siguiente router. Los atributos

atraviesan el router sin ser cambiados, si no son reconocidos.

- **INTRANSITIVO OPCIONAL.** Estos atributos son eliminados si caen en un router que no entiende o reconoce los atributos. Estos atributos no serán propagados al peer BGP.

A continuación, se describen los atributos más importantes:

ORIGIN (código de tipo 1

Atributo bien conocido y obligatorio, que contiene información referente al mecanismo por el cual se obtuvo la información en el AS donde fue generada.

Las posibilidades son “IGP”, “EGP” o “INCOMPLETE”.

- **0: IGP**: Indicado con una **i**, presente si la ruta se ha aprendido con el comando network.
- **1: EGP**: Indicado con una **e**, presente si la ruta ha sido aprendida desde otro AS.
- **2: INCOMPLETE**: Indicado con un **?**, aprendido de una redistribución de la ruta.

AS_PATH (código de tipo 2)

Es un atributo bien conocido y obligatorio, que contiene una lista de la secuencia de AS’s a través de los cuales ha pasado la notificación de ruta. Este atributo es utilizado por BGP para evitar bucles, además de ofrecer información muy valiosa para aplicar políticas.

NEXT_HOP (código de tipo 3)

Es un atributo bien conocido y obligatorio que contiene la dirección IP del enrutador al que se envía tráfico para la ruta.

MULTI_EXIT_DISC (MED, código tipo 4)

Es un atributo opcional y no transitivo. MED es una métrica para aquellas rutas en las que hay múltiples vínculos entre AS's (un AS configura el MED y otro AS lo utiliza para elegir una ruta).

LOCAL_PREF (código de tipo 5)

Es un atributo bien conocido utilizado en I-BGP para informar sobre la preferencia entre múltiples rutas disponibles para un mismo prefijo.

ATOMIC_AGGREGATE (código de tipo 6)

Es un atributo bien conocido que informa de un suceso de agregación de la información de rutas a lo largo del camino, por lo que se ha eliminado parte de la información en el AS_PATH.

AGGREGATOR (código de tipo 7)

Es un atributo opcional y transitivo usado para identificar el AS que ha realizado la agregación de la información de ruta contenida.

COMMUNITY (código de tipo 8)

Es un atributo opcional y transitivo definido posteriormente en la RFC 1997 [RFC1997] que se usa para marcar la información de rutas para su posterior procesamiento.

PESO

Atributo especial de Cisco y es usado para el proceso de selección de una ruta. Es local en el enrutador y no se propaga en los anuncios de ruteo. Rutas con mayor peso son preferidas. Por default, el peso es de 32768 para rutas que se originan en el enrutador y 0 para otras rutas.

3.7 SELECCIÓN DE RUTA Y MANIPULACION DE ATRIBUTOS

3.7.1 SELECCIÓN DE RUTA

Las rutas son intercambiadas entre iguales BGP mediante mensajes UPDATE ejecutando políticas o filtros sobre las actualizaciones, y luego pasa las rutas a otros iguales BGP.

Se requiere una implementación para guardar todas las actualizaciones BGP en una tabla de enrutamiento BGP separada de la tabla de enrutamiento IP. Si existen muchas rutas hacia el mismo destino, BGP no inundará sus iguales con todas esas rutas; en su lugar, tomará la mejor ruta y la enviará.

Las rutas locales validas originadas en el sistema y las mejores rutas aprendidas de los iguales BGP son instaladas posteriormente en la tabla de enrutamiento IP. La tabla de enrutamiento IP es la decisión final de enrutamiento y se utiliza para poblar la tabla de reenvío.

El modelo involucrará los siguientes componentes:

- Un conjunto de rutas que el router recibe de sus iguales.
- Un motor de políticas de entrada que pueda filtrar las rutas o manipular sus atributos.
- Un proceso de decisión que decide que rutas utilizará el propio router.
- Un conjunto de rutas que el mismo router utiliza.
- Un motor de políticas de salida que puede filtrar las rutas o manipular sus atributos.
- Un conjunto de rutas que el router publica a otros iguales.

La Figura 3.5, ilustra este modelo. La explicación posterior proporciona más detalles sobre cada componente.

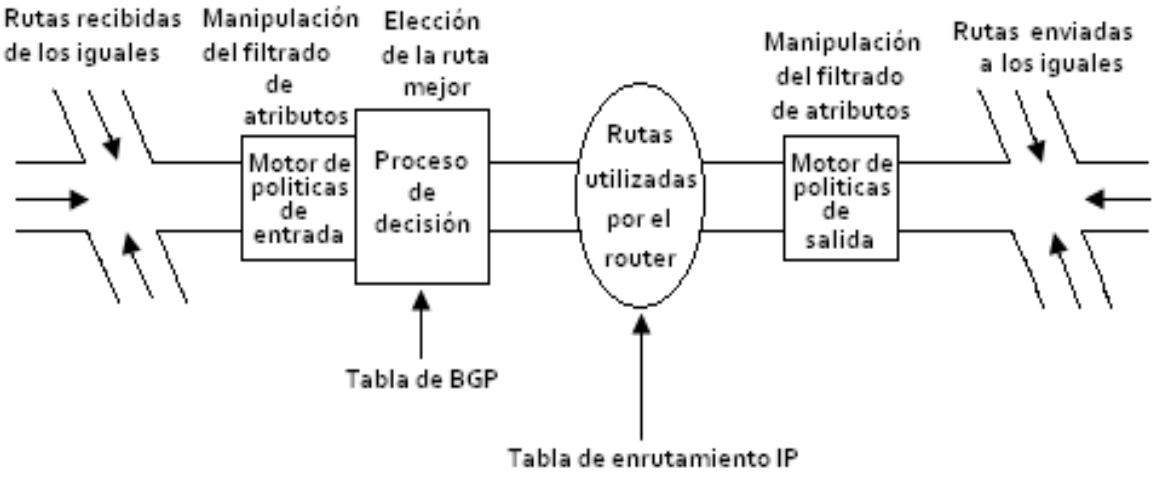


FIGURA 3.25 Visión general del proceso de enrutamiento

FUENTE: http://www.potaroo.net/tools/ipv4

BASES DE INFORMACIÓN DE ENRUTAMIENTO DE BGP.

La tabla de enrutamiento BGP consta de tres partes distintas: Adj-RIB-In, Loc-RIB y Adj-RIB-Out.

Adj-RIB-In: esta disponible como entrada al proceso de decisiones BGP después de ser manipuladas o incluso filtradas por el motor de políticas de entrada asociada con el igual.

Loc-RIB: es el resultado del proceso de decisión de BGP después de haber aplicado las políticas locales entrantes por el motor de políticas de entada.

Adj-RIB-Out: contiene la información del Loc-RIB para ser publicada al igual después de haber aplicado el motor de políticas de salida.

Rutas recibidas desde iguales.- recibe rutas desde iguales externos y / o internos mediante mensajes UPDATE.

Motor de políticas de entrada.- administra el filtrado de rutas y la manipulación de atributos. El filtrado se realiza basándose en diferentes parámetros como los prefijos IP, AS_PATH y otros valores de atributos BGP.

BGP también utiliza el motor de políticas de entrada para manipular los atributos de la ruta a fin de influir en su propio proceso de decisión y, por tanto, afecta a las rutas que se utilizarán realmente para llegar a un destino dado.

Rutas utilizadas por el router.- Las mejores rutas, como las identificadas por el proceso de decisión, se sitúan el Loc-RIB.

Esas rutas se convierten en candidatas que pueden ser publicadas a otros iguales o situadas en la tabla de enrutamiento IP. Si una ruta no esta situada en el Loc-RIB, no puede colocarse en el Adj-RIB-Out para su publicación a los iguales.

Motor de políticas de salida.- éste es el mismo motor que el motor de políticas de entrada aplicado al lado de la salida. Las rutas utilizadas por el router (las mejores rutas) además de las rutas que el router genera localmente son entregadas a este motor para su procesamiento.

3.7.1.1 PROCESO DE DESICIÓN DE BGP

Cuando existen múltiples rutas para un mismo prefijo, BGP debe elegir una de ellas para incluirla en la tabla de rutas que efectivamente será utilizada por el router.

Para ello, se utilizan una serie de reglas que se describirán a continuación. Las reglas siguientes son aplicadas en orden y solamente hasta que una de ellas seleccione una ruta sobre otra.

1. Preferir el WEIGHT (peso) mayor (el peso es una parámetro propietario de Cisco, local al router).
2. Si los pesos son iguales, prefiere la ruta con mayor (Preferencia local) LOCAL_PREFERENCE.

3. Si no hay rutas originadas localmente y la preferencia local es la misma, prefiere la ruta con el AS_PATH más corto.
4. Si la longitud del AS_PATH es la misma, prefiere la ruta con el tipo de ORIGIN (origen) más bajo (donde IGP es más bajo que EGP, y EGP es más bajo que INCOMPLETE).
5. Si el tipo de origen es el mismo, prefiere la ruta con el valor MED más bajo si las rutas fueron recibidas del mismo AS.
6. Si las rutas tienen el mismo valor MED, prefiere las rutas EBGP a las rutas IBGP.
7. Si todos los escenarios precedentes son idénticos, prefiere la ruta que puede ser alcanzada mediante el vecino IGP más próximo hasta llegar a la ruta más corta que es el NEXT_HOP de BGP.
8. Se prefiere el path con el vecino BGP que tenga el Router ID más bajo.
9. Se prefiere el camino con el vecino BGP que tenga la dirección IP más baja.

Nota:
Cabe notar que algunas de las reglas arriba detalladas no están recogidas en la RFC 1771 que define BGP, pero sin embargo son habitualmente usadas en las implementaciones comerciales.

3.7.2 MANIPULACIÓN DE ATRIBUTOS EN BGP

Si una ruta es permitida, sus atributos pueden ser modificados para afectar al proceso de decisión (en el mismo AS o en los vecinos). Como se verá posteriormente, la manipulación de atributos es clave para establecer las políticas de enrutamiento, el equilibrado de la carga y la simetría de ruta.

3.7.2.1 MANIPULACIÓN ATRIBUTO AS_PATH

Un AS malicioso puede falsear los atributos de camino (AS_PATH) de un mensaje UPDATE, modificando, quitando o insertando AS's en él, o cambiando el orden de los AS's (creando retardos, modificando patrones de tráfico).

El ejemplo 3.1, muestra como se puede manipular la información AS_PATH para conseguir que AS_PATH sea más largo añadiendo al final números AS a la ruta

Ejemplo 3.1.

Manipulación del atributo AS_PATH

```
router bgp 27919
network 192.68.11.0
neighbor 172.16.20.2 remote-as 19582
neighbor 172.16.20.2 route-map PRUEBA out
network 192.68.6.1 remote-as 23216
no auto-summary

route-map PRUEBA permit 10
set as-path prepend 27919 27919
```

3.7.2.2 MANIPULACIÓN DEL ATRIBUTO MED

Es un atributo usado para el proceso de selección de una ruta. También llamado "métrica", es una indicación a vecinos externos acerca del camino preferido para entrar en el AS desde afuera.

Esto puede producir que se vea disminuida la ingeniería de tráfico y las políticas de enrutamiento.

Por defecto el valor del MED es 0 y cuanto más bajo sea el valor es más preferible. Como se puede observar en el ejemplo 3.2, describe el proceso de manipulación del atributo MED.

Ejemplo 3.2.

Manipulación del atributo MED

```
router bgp 27814
neighbor 192.68.5.2 route-map PRUEBA1 out

route-map PRUEBA1 permit 10
set metric 200
```

Cisco además, ha añadido dos funcionalidades nuevas al MED que permiten realizar comparaciones:

- **bgp deterministic-med** compara valores de MED en las rutas anunciadas por diferentes peers del mismo AS
- **bgp always-compare-med** compara el atributo MED de diferentes ASs para seleccionar el path más adecuado

3.7.2.3 MANIPULACIÓN DEL ATRIBUTO COMMUNITY

El atributo communities es un atributo global opcional y transitivo y es un número en el rango 1 - 4.294.967.200.

Las comunidades más comunes son:

- **no-export**: No anuncia esta ruta a otros peers Ebgp
- **no-advertise**: No anuncia esta ruta a ningún peer

La configuración del ejemplo 3.3, muestra que se ha definido un mapa de ruta SEND-COMMUNITY hacia su vecino. La instancia 10 del mapa de ruta corresponderá al prefijo y establecerá su atributo de comunidad a **no-export.**

Ejemplo 3.3.

Manipulación del atributo COMMUNITY

```
router bgp 27814
neighbor 172.16.20.1 remote-as 23216
neighbor 172.16.20.1 send-community
neighbor 172.16.20.1 route-map PRUEBA2 out
!
route-map PRUEBA2 permit 10
match ip address 10
set community no-export
!
route-map PRUEBA2 permit 20
```

3.7.2.4 MANIPULACIÓN DEL ATRIBUTO NEXT_HOP

Este atributo indica la dirección IP del siguiente salto eBGP que se va a utilizar para alcanzar el destino. Para definir el siguiente salto como el vecino en si, se usará el comando **next-hop-self**. (Ver ejemplo 3.4)

Ejemplo 3.4.

Manipulación del atributo NEXT-HOP

```
router bgp 27814
neighbor 172.16.2.35 remote-as 23216
neighbor 172.16.2.35 next-hop-self
```

3.7.2.5 MANIPULACIÓN DEL LOCAL_PREFERENCE

El atributo local preference indica cual es el camino para salir del AS local, este atributo no se pasará a vecinos eBGP. Por defecto en routers Cisco es 100 y se prefiere la local preference más grande.

El ejemplo 3.5, muestra el proceso de manipulación del atributo LOCAL PREFERENCE para que tenga una preferencia local más alta para todas las actualizaciones BGP.

Ejemplo 3.5.

Manipulación del atributo LOCAL PREFERENCE

```
router bgp 27814
neighbor 192.68.5.2 remote-as 19582
neighbor 192.68.5.2 route-map PRUEBA in
route-map PRUEBA permit 10
set local-preference 300
bgp default local-preference 300
```

3.8 BGP CON IPv6

Configurar BGP sobre IPv6 es parecido a IPv4.

- Debe existir una ruta en la tabla de enrutamiento para que se publique vía BGP.
- Hay que crear el peering con el equipo remoto.
- Colocar filtros correspondientes tales como filtros entrantes y salientes.

Antes de crear la sesión BGP hay que conocer:

- Dirección IPv6 local.
- Subred IPv6 a publicar.
- Dirección IPv6 remota.
- Password (opcional).

Un ejemplo de configuración de BGP sobre IPv6 sería:

```
router bgp 65501
bgp log-neighbor-changes
neighbor 2820:22:1:1::1 remote-as 1111
neighbor 2820:22:1:1::1 update-source POS3/0
!
address-family ipv6
neighbor 2820:22:3:1::1 activate
network 2820:26::/32
```

En caso de levantar sobre el mismo enlace una sesión BGP en IPv4 es necesario también el siguiente comando:

```
address-family ipv4
neighbor 2820:22:3:1::1 activate
```

3.9 COMANDOS DE CONFIGURACIÓN DE BGP SOBRE EQUIPAMIENTO MARCA CISCO

Los apéndices de esta parte de la tesis proporcionaran referencias adicionales para un estudio más detallado, una referencia actualizada de comandos BGP del IOS de Cisco. (Ver anexo 2)

CAPÍTULO 4.

PROCESO DE TRANSICIÓN

IPv6 e IPv4 coexistirán durante muchos años. Una amplia gama de técnicas se han definido que permiten la coexistencia y proporciona una transición fácil.

Este capítulo describe las principales técnicas disponibles y factibles de implementar hoy en día y conforme IPv6 siga creciendo en nuestras redes, se definirán nuevas herramientas y mecanismos para que la transición sea fácil de realizar.

4.1 Mecanismos de Transición de IPv4 a IPv6

No es previsible que IPv6 se despliegue de manera rápida. Actualmente existe una gran infraestructura IPv4 extendida y funcionando, y, por lo tanto, el despliegue de IPv6 debe ser tan poco disruptivo como sea posible.

Esto significa que, aunque IPv4 e IPv6 no son compatibles, deberán coexistir por un periodo de tiempo indeterminado. Los mecanismos de transición proporcionan comunicación entre nodos IPv4 e IPv6, y aunque IPv6 se han definido varios, la IETF se está centrando en unos pocos.

Como premisa al diseño de IPv6, se especificó que el nuevo protocolo debía coexistir con el actual (IPv4). Para ello, se desarrollaron los llamados "mecanismos de transición". Los mismos que se dividen en 3 grupos:

- **Técnicas Doble Pila.** Permiten a IPv4 y a IPv6 coexistir en los mismos dispositivos y redes.
- **Técnicas de Túnel.** Permiten el transporte de tráfico de IPv6 a través de la infraestructura de IPv4 existente.
- **Técnicas de Traducción.** Permiten comunicar solamente nodos IPv6 con nodos IPv4.

4.1.1 MECANISMO DOBLE PILA (IPv4 A IPv6)

Este mecanismo, como su nombre lo indica, se refiere al uso de dos pilas, de diferente protocolo, que trabajan paralelamente y permiten al dispositivo trabajar vía ambos protocolos.

Todos los sistemas operativos modernos soportan IPv6 (windows XP/2003/vista, Windows 7[15], Linux, BSD, IOS de Cisco[16]). Añadir IPv6, no elimina la pila IPv4.

Las aplicaciones escogen la versión de IP a utilizar, por ejemplo en función de la respuesta DNS[17] (destino con registro AAAA[18] usa IPv6, caso contrario IPv4). Ver Figura 4.1.

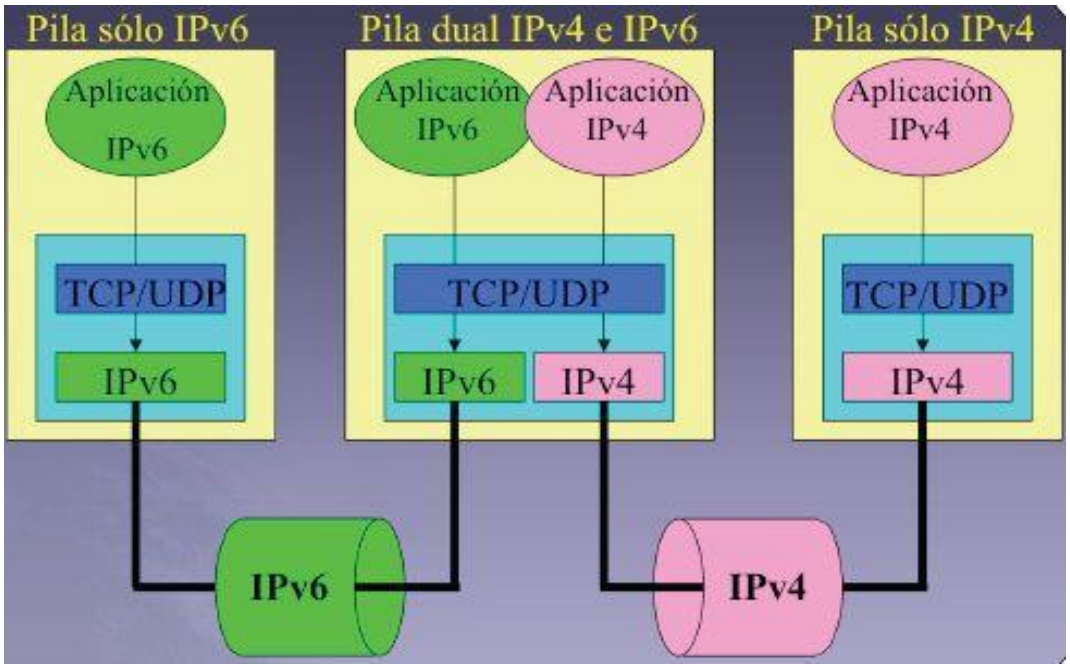


FIGURA 4.26 Mecanismo Doble Pila
Fuente: http://www.aeprovi.org.ec

15. Incluye numerosas actualizaciones, entre las que se encuentran avances en reconocimiento de voz, táctil y escritura, soporte para discos virtuales, mejor desempeño en procesadores multi-núcleo, mejor arranque y mejoras en el núcleo.

16. Es un paquete de routing, switching, interconexión y las funciones de telecomunicaciones estrechamente integrado con una multitarea del sistema operativo.

17. Domain Name System o en español: sistema de nombre de dominio es una base de datos distribuida y jerárquica la misma que almacena información asociada a nombres de dominio en redes como Internet.

18. Los registros AAAA almacenan direcciones de 128 bits pertenecientes a la versión 6 de IP (IPv6). Se utilizan para asociar un nombre de host con un dominio y especifica la dirección IPv6 asignada al host.

4.1.2 MECANISMO DE TÚNEL

Se encapsulan paquetes IPv6 dentro de paquetes IPv4; los paquetes resultantes viajan sobres redes IPv4.

Permite la creación de un solo salto IPv6 aunque hayan varios IPv4, lo cual, se conoce comúnmente como enlace punto a punto.

Las direcciones IPv6 de ambos extremos del túnel pertenecen al mismo prefijo.

Varias opciones cada una con diferente tipo de encapsulación.

Como se observa en la Figura 4.2, los routers que se encuentran localizados en los extremos de la isla son doble pila.

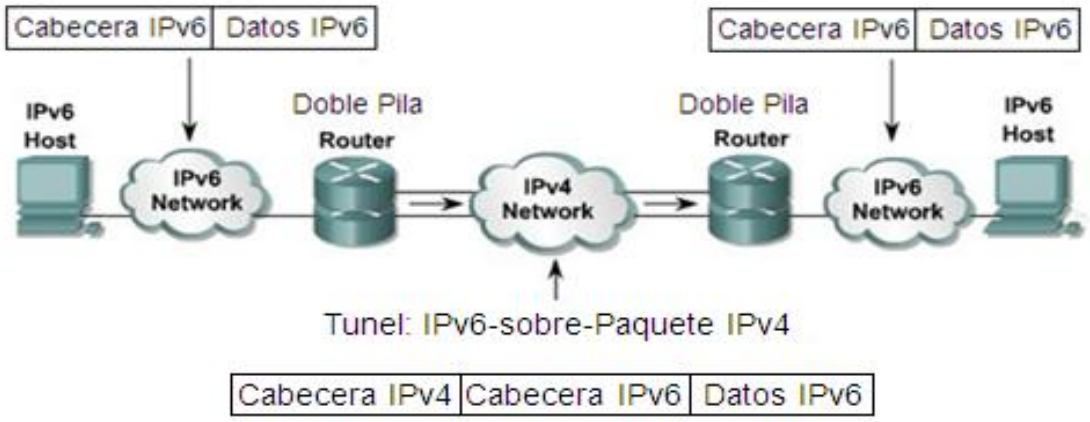


FIGURA 4.27 Mecanismo de Túnel
Fuente: http://www.aeprovi.org.ec

4.1.2.1 TÚNELES 6TO4

Permite implementación rápida de IPv6 sin requerir asignaciones de los RIR o ISPs.

Este método requiere un código especial en los routers de borde, pero los hosts y routers dentro de la isla IPv6 no requieren soporte 6to4.

Asigna un prefijo IPv6 válido a cada isla IPv6. Cada una recibe un prefijo /48 dentro del rango 2002::/16. El prefijo asignado es una concatenación de 0x2002 y la dirección IPv4 del router de borde en formato hexadecimal. Cuando un paquete IPv6 con una dirección destino en el rango 2002::/16 alcanza un router de borde 6to4, el router extrae la dirección IPv4 embebida en la dirección destino (insertada entre el 3º y 6º octetos). Entonces el router 6to4 encapsula el paquete IPv6 en un paquete IPv4 con dirección destino la dirección IPv4 extraída que representa la dirección de otro router de borde.

Como se observa en la Figura 4.3, en el otro extremo el router 6to4 desencapsula el paquete y lo reenvía hacia la dirección destino original IPv6.

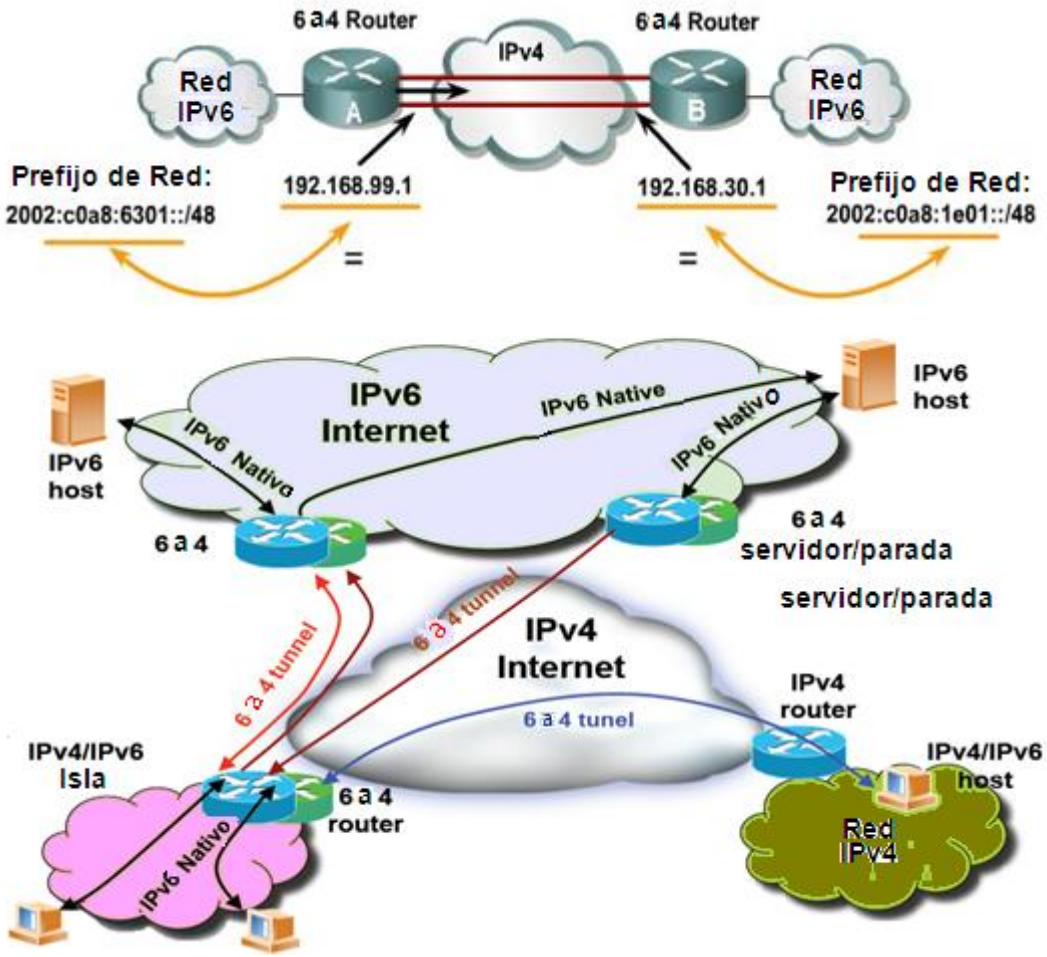


FIGURA 4.28 Túnel 6to4
Fuente: http://www.aeprovi.org.ec

4.1.2.2 TEREDO

- Denominado originalmente Shipworm

- Está pensado para proporcionar IPv6 a nodos que están ubicados detrás de NAT.

- El encapsulamiento de los paquetes IPv6, se los hace mediante paquetes UDP[19]/IPv4.

- Intervienen varios agentes, como se muestra en la Figura 4.4:
  - Teredo de servicio (Teredo server).
  - Teredo de parada (Teredo relay).
  - Teredo de cliente (Teredo client).

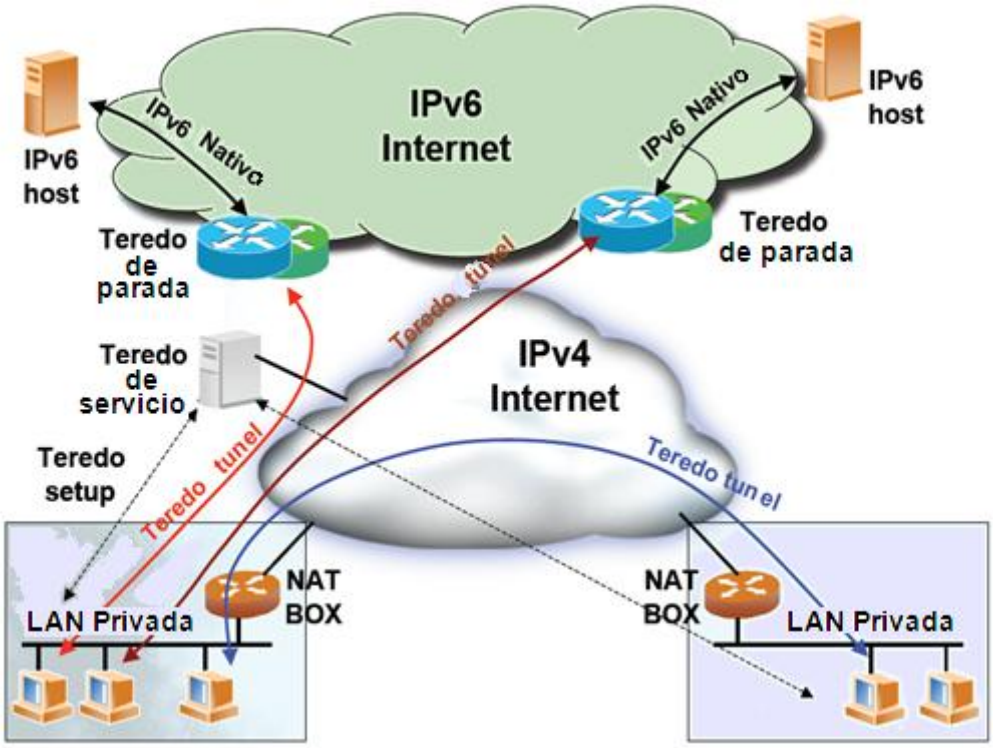


FIGURA 4.29 Conexión mediante Teredo
Fuente: http://www.aeprovi.org.ec

19. User Datagram Protocol es un protocolo del nivel de transporte basado en el intercambio de datagramas.

- El cliente configura un Teredo server que le asigna una dirección IPv6 dentro del rango 2001:0000::/32 basándose en la dirección IPv4 pública y el puerto usado. Con esto el cliente ya tiene conectividad a otros clientes Teredo.

- Para conectividad al resto del mundo IPv6 se requiere un Teredo relay (puede ser el mismo equipo Teredo server).

- Microsoft proporciona Teredo servers públicos y gratuitos, pero no Teredo relays.

4.1.2.3

Como muestra la Figura 4.5, los túneles broker requieren configuración de los equipos en ambos extremos del túnel.

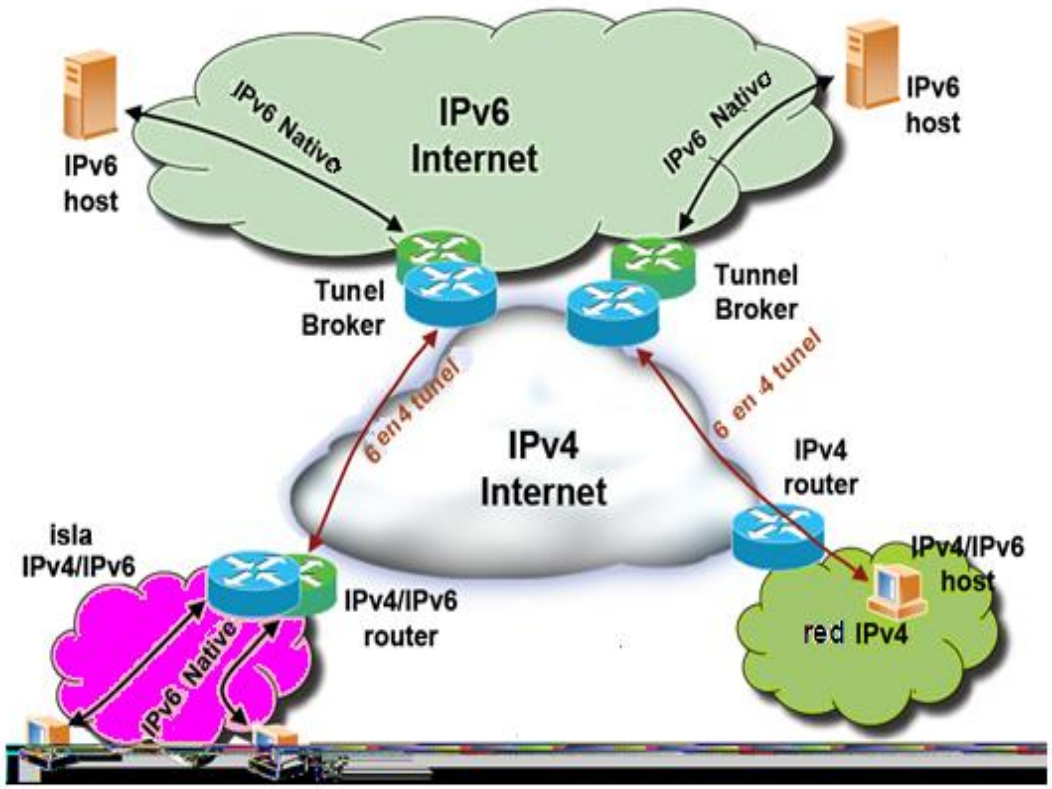


FIGURA 4.30 Conexión mediante Túnel Broker
Fuente: http://www.aeprovi.org.ec

Un TB es un intermediario que permite a usuarios finales crear un túnel para conectarse al resto del mundo IPv6.

El procedimiento es el siguiente:

- El usuario solicita al TB la creación de un túnel a través de una interfaz web
- El TB le asigna una dirección IPv6 y le proporciona instrucciones para configurar el túnel en el lado del usuario.
- El TB configura el router que representa, para el usuario, el extremo opuesto del túnel.

4.2 MECANISMOS DE TRADUCCIÓN

Es una extensión de las técnicas NAT, la más común es NAT-Protocol Translation (NAT-PT)[20].

Al observar la Figura 4.6, se ve que un nodo intermedio (traductor) traduce paquetes IPv6 en IPv4 y viceversa, utilizando reglas de traducción configuradas estáticamente (modifica las cabeceras).

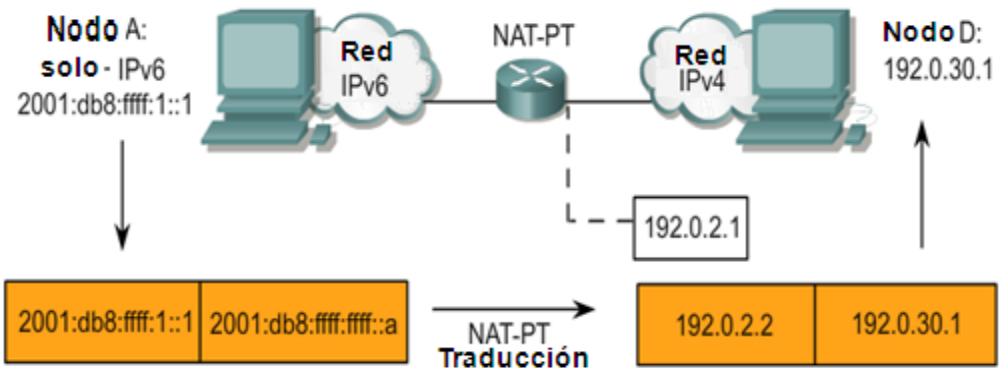


FIGURA 4.31 Mecanismo de Traducción
Fuente: http://www.aeprovi.org.ec

20. Obras de captación, traducción y el envío de paquetes desde el IPv6 para la red IPv4 (y viceversa).

Puede servir para conectar nodos IPv6-only con nodos IPv4-only.

Con muchos host la tabla de traducción puede ser grande.

La traducción puede tener un mapeo dinámico con DNS AGL (DNS Application Level Gateway)[21].

No es recomendable pues la traducción no es perfecta.

4.2 MECANISMO QUE MEJOR SE ADAPTA A BGP

Es una realidad que la transición a IPv6 es inminente, las direcciones IPv4 se están acabando y a partir de ahí la solución es IPv6.

Hace años atrás se escuchaba hablar de que las direcciones se acabarían pero muy pocos pensaban en la masificación de las redes y comunicaciones, así que el futuro es ahora y en pocos meses o años (todo depende del escenario de cada empresa) nos tocará migrar a IPv6 si no es que ya lo han hecho.

Este es un tema en el que hay que profundizar bastante, tanto en teoría como en la práctica; por eso que, desde que se tiene conocimiento sobre algunos mecanismos de transición de IPv4 a IPv6, se tomo en cuenta que no hay un mecanismo que mejor se ajuste sino mas bien hay mecanismos que se pueden utilizar dependiendo de las necesidades de la red.

Pero en el caso de **NAP.EC** el mecanismo que mejor se adapta a BGP el de Doble Pila, tal vez no por ser una solución elegante, sino más bien por ser el más utilizado en los procesos de migración por su transparencia y fácil implementación. Tal es así, que los sistemas operativos han comenzado a activar ambas pilas de protocolos en el mismo equipo, es decir, el equipo debe tomar la decisión de qué tipo de conexión utilizará, estas pilas correrán de manera independientes.

---

21. Pasarela DNS de Nivel de Aplicación ayuda a traducir los mapeos Nombre-Dirección-Privada en las cargas útiles DNS en mapeos Nombre-Dirección-Externa y viceversa, usando la información de estado disponible en NAT.

Como el nombre lo dice tener dos pilas, envuelve el instalar tanto la pila IPv4 como el IPv6 en un host. Esto significa que el host puede tomar decisiones acerca de cuándo las conexiones deben hacerse usando IPv4 o IPv6; generalmente esto se hace basándose en la disponibilidad de la conectividad IPv6 y los registros DNS. Las pilas IP e IPv6 pueden y usualmente serán completamente independientes, pues las interfaces pueden enumerarse de forma separada, habilitar y deshabilitarlas separadamente y esencialmente tratadas como máquinas separadas.

Con este mecanismo, se pretende lograr que toda la red permita encaminar paquetes IPv4 e IPv6 internamente. Su implementación será posible en casi la totalidad de host y servidores internos, pues los sistemas operativos presentes, dígase familia de Windows (XP, 2003 Advenced Server, 2000, 98) admiten el uso de doble pila. En general este será el mecanismo principal a aplicar en la primera etapa de migración y sobre el cual se sustentan todas las acciones a desarrollar de forma práctica.

4.3 COMANDOS DE CONFIGURACIÓN IPv6 SOBRE EQUIPAMIENTO MARCA CISCO.

El anexo 3 describe la utilización de sintaxis de cada uno de los comandos que se usan para configurar y supervisar IPv6.

CAPÍTULO 5.

ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA RED

En el Capitulo 5, se explica el análisis de la situación actual de la red, topología de la red, políticas de seguridad, peering y enrutamiento.

El NAP.EC consiste en una infraestructura instalada con el objetivo de de intercambiar trafico de Internet originado y terminado en el Ecuador, y es administrada por la **AEPROVI** (Asociación de Empresas Proveedoras de Servicios de Internet, Valor Agregado, Portadores y Tecnologías de la información).

Encargado de la administración del NAP.EC de forma imparcial y sin fines de lucro; entre sus funciones está brindar soporte técnico y velar por el cumplimiento de los compromisos asumidos por los participantes. La asociación fue creada con domicilio en la ciudad de Quito, nacionalidad ecuatoriana e ingerencia a nivel nacional.

Creada el 1 de marzo del año 2000, los representantes legales de 8 empresas (Megadatos S.A., Ramtelecom Telecomunicaciones S.A., Satnet S.A., Impsatel del Ecuador S.A., Servicios Cyberweb S.A., Infornetsa S.A., Satefar S.A. y Prodata S.A.) decidieron organizarse en una asociación que vele por los intereses del sector de telecomunicaciones. Actualmente cuenta con la participación de 25 socios.

NAP.EC tiene cobertura nacional, para lo cual AEPROVI se encarga de implementar y habilitar los nodos que sean necesarios conforme a los requerimientos de intercambio de tráfico local. Para participar de NAP.EC no es necesario ser socio de AEPROVI.

También se brinda coubicación a infraestructuras de aplicaciones que le den valor agregado al intercambio de tráfico local, por ejemplo los servidores de nombres de dominio de NIC.EC y del Root Server F.

5.1 TOPOLOGÍA DE LA RED

En Ecuador los ISPs facultados para el intercambio de tráfico en el NAP, deben estar autorizados para prestar el servicio de Internet conforme la legislación vigente, además de tener un número de sistema autónomo público y direccionamiento IP propio. En lo que respecta al acceso, los ISPs pueden usar las facilidades de transporte de su red o usar las facilidades de terceros para llegar físicamente al NAP.

Es responsabilidad de cada proveedor realizar la instalación y posterior mantenimiento de su enlace de acceso al NAP Ecuador, para conectarse a esta infraestructura deberán utilizar interfaces ethernet de 10, 100 o 1000Mb/s (se aplica a conexiones nuevas). Con respecto a la arquitectura, en lo referido a la infraestructura física, ésta cuenta con dos nodos, no interconectados entre si, uno de ellos presente en la ciudad de Guayaquil y el otro en Quito (Ver Figura 5.1).

FIGURA 5.32 Nodos de Intercambio de Tráfico en Ecuador
Fuente: http://www.aeprovi.org.ec

Cada nodo tiene una infraestructura híbrida de capa 2 y capa 3 (L2/L3), donde en el core del mismo se tiene un switch Cisco Catalyst 3560G-24TS y un router Cisco 7200VXR como reflector de rutas.

El intercambio es realizado por medio de peering abierto multilateral, permitiéndose la realización de peerings bilaterales entre los miembros.

Los participantes comparten un medio Ethernet y las sesiones BGP en cada nodo se levantan entre un servidor de rutas (ruteador de NAP.EC) y los respectivos ruteadores de borde de cada proveedor. Los nodos de NAP.EC están unidos mediante un enlace interurbano que transporta el tráfico entre dichas ciudades.

Como se muestra en la Figura 5.2, actualmente, la topología física de NAP.EC es la siguiente:

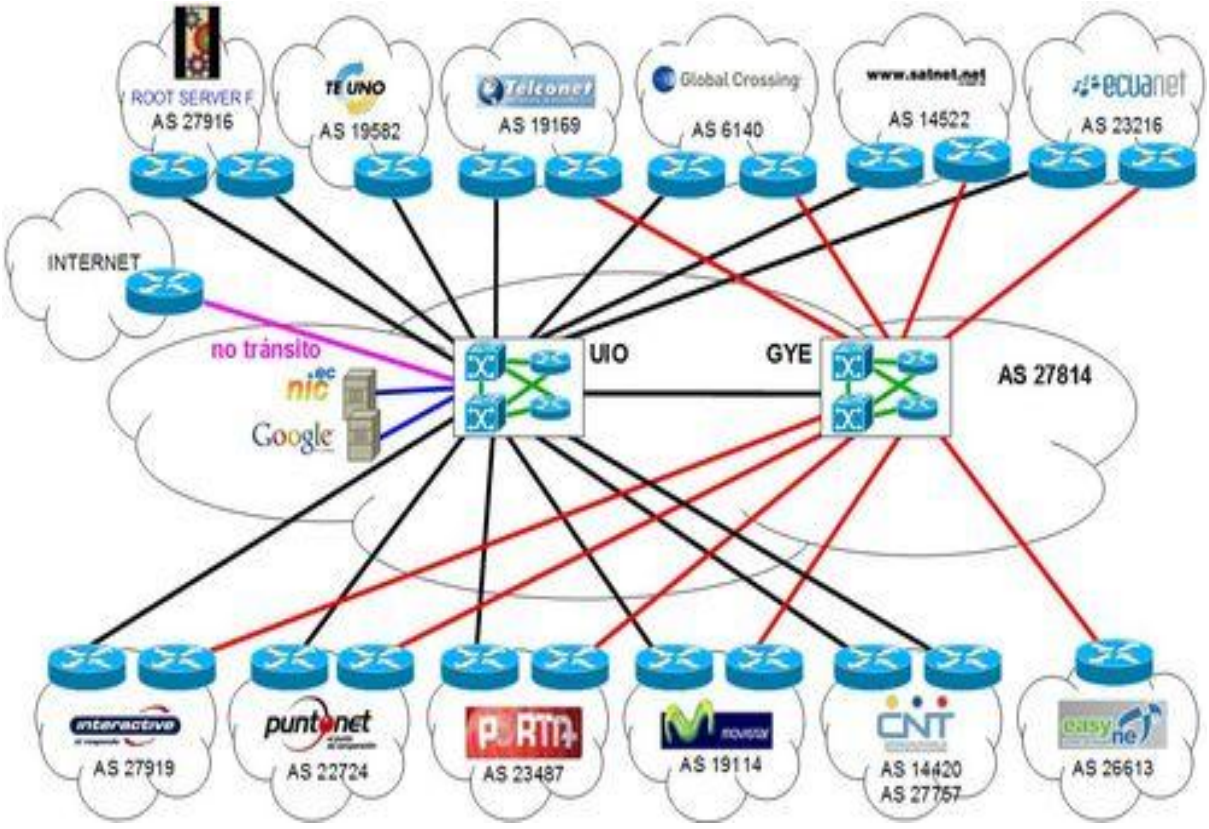


FIGURA 5.33 Topología del NAP
Fuente: http://www.aeprovi.org.ec

5.1.1 NAP

Es un switch de alta velocidad o bien una red de switches, a los que pueden estar conectados un cierto número de routers para intercambiar tráfico. Los NAP deberían trabajar a la máxima velocidad permitida por las características técnicas de los switches y debe ser posible actualizarlos según lo solicite la demanda y el uso. El NAP puede ser tan simple como un switch Ethernet/fastethernet (10/100 Mbps) o como un switch ATM (normalmente 45 Mbps) pasando tráfico de un proveedor a otro.

Los NAPs están tradicionalmente gestionados por organizaciones independientes y sin ánimo de lucro en el negocio de Internet. A diferencia de Cuba y Chile que son países en los cuales cada gobierno es el encargado de administrar el NAP.

Dependiendo de las políticas de cada NAP se puede, o no, comercializar servicios en ellos o intercambiar tráfico internacional. Los ISP´s pagan una cuota de socio por adherirse al NAP más los costes asociados al alojamiento de equipos y la puerta física a la red del NAP.

5.2 ENRUTAMIENTO Y TRÁFICO

5.2.1 ENRUTAMIENTO

Es la conmutación de paquetes de una red a otra. La idea del enrutamiento está estrechamente ligada a las redes y subredes (IP, IPX, etc.) y al hecho de que los enrutadores son los separadores de esas redes/subredes.

La base de todas estas decisiones es la tabla de enrutamiento, una especie de base de datos sobre las rutas que dice justamente esa información: por dónde se está más cerca de una red en particular. La tabla de enrutamiento es la información que usa el enrutador efectivamente, es decir, aún si están configuradas ciertas rutas eso no significa que tengan que aparecer en la tabla de enrutamiento, pero si

está en la tabla de enrutamiento eso sí va a ser lo que sucede con los paquetes destinados a una red de las que están en la tabla.

5.2.2 PEERING (INTERCAMBIO DE TRÁFICO)

El peering consiste en un acuerdo bilateral suscrito por dos operadores o ISP para intercambiar tráfico de sus propios clientes en pura reciprocidad, es por tanto una variante de interconexión por capacidad; generalmente no conlleva pagos entre los operadores.

5.2.2.1 ACUERDO DE INTERCAMBIO DE TRÁFICO Y TRÁNSITO

Existe una serie de acuerdos de intercambio de tráfico y de tránsito que permiten la interconexión:

5.2.2.1.1 ACUERDO DE INTERCAMBIO DE TRÁFICO PRIVADO BILATERAL

Dos ISP negocian una interconexión bilateral y "privada" haciendo uso de una o dos líneas dedicadas con el fin de intercambiar el tráfico entre sus respectivas redes. Este tipo de conexión se denomina peering (entre pares) porque la interconexión se produce en un mismo nivel de la jerarquía de la red, es decir, cuando los ISP son homólogos. Por lo general, estos intercambios son gratuitos, aunque no siempre: el tráfico de los ISP no es facturado, pero los gastos en que incurren son divididos.

Los ISP que establecen acuerdos por modalidad de peering suelen ser del mismo tamaño, a fin de evitar desequilibrios en sus flujos de tráfico respectivos. Por consiguiente, los ISP locales (Nivel 3) de tamaño similar establecerán acuerdos por modalidad de peering, e igualmente harán los ISP nacionales o regionales de dimensiones equivalentes y los proveedores de backbone. El tamaño de un ISP se determina mediante el número de clientes que tiene, el volumen de tráfico, la capacidad del backbone y el alcance geográfico de su red, así como el número de sitios Web de contenido.

5.2.2.1.2 ACUERDO DE INTERCAMBIO DE TRÁFICO MULTILATERAL

El uso compartido de las instalaciones es beneficioso para un gran número de ISP, ya que intercambian el tráfico con el mayor número de redes posible. Esto permite el uso simultáneo por modalidad de peering entre dos o más ISP de nivel 3. Existen dos modalidades:

- *Punto de interconexión de Internet (IXP):* Para conseguir una interconexión óptima los ISP buscan establecer puntos de presencia (POP)[22] o incluso situar sus servidores próximos entre sí.

- *Puntos de acceso a la red (NAP):* Los NAP tienen dos funciones distintas. Por una parte actúan como un proveedor de intercambio entre los ISP de nivel 3 que buscan acuerdos bilaterales por modalidad de peering (una IXP) y, por otro, actúan conforman una plataforma en la que los ISP de nivel 3 alcanzan acuerdos con uno o más proveedores de backbone de Internet que también están conectados a los NAP. De este modo los ISP de nivel 3 consiguen acceso a las redes de los proveedores de backbone (IBP).

5.2.2.1.3 ACUERDOS DE TRÁNSITO

En un acuerdo de tránsito, un ISP paga a otro, en relación cliente-proveedor, para que éste transporte el tráfico de aquél. "Cuando existe un acuerdo de servicio mayorista o minorista, un ISP es en efecto el cliente de otro ISP". "En esta relación el ISP cliente (más alejado de la conexión global) adquiere un servicio de tránsito y conectividad del ISP proveedor (más cercano a la conexión global)". Al ser empresas, los IBP establecen gratuitamente acuerdos por modalidad de peering pero facturan a otros ISP de los niveles 3 y 2 por el acceso a su red.

Las negociaciones no son solamente horizontales, entre ISP, sino que también se realizan verticalmente entre los 'pequeños ISP locales' y los 'grandes ISP nacionales'.

---

22. En clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto. Es un protocolo de nivel de aplicación en el Modelo OSI.

5.2.3 MONITOREO DE TRÁFICO - NAP.EC

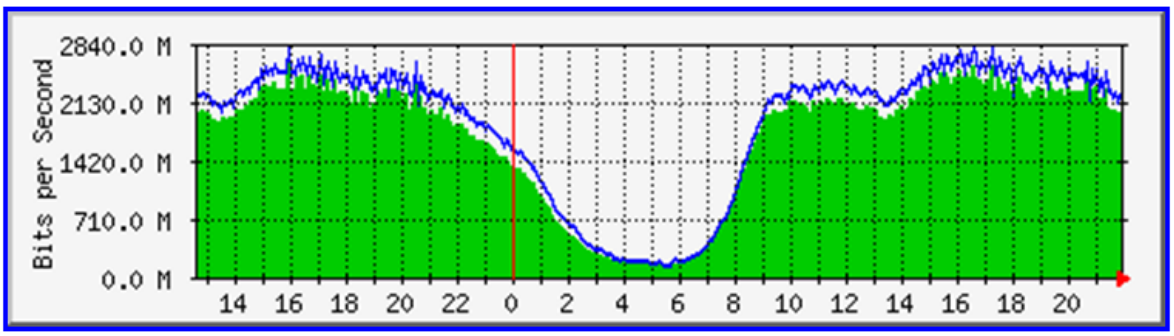
NAP.EC, para monitorizar la carga de tráfico sobre determinados nodos de la red utiliza la herramienta llamada MRTG (Multi Router Traffic Grapher), esta permite supervisar el tráfico de interfaces de red generando páginas HTML con gráficos que proveen una representación visual de este tráfico. MRTG es un software configurado para que se recopilen datos cada 5 minutos pero el tiempo puede ser modificado. Mediante esta herramienta se puede tomar muestras de tráficos de los clientes, ya sea por horas, días, semanas, o meses, etc.

Las siguientes gráficas, muestran las estadísticas y tasas de transferencia del tráfico NAP.EC, las mismas que se actualizan cada 5 minutos.

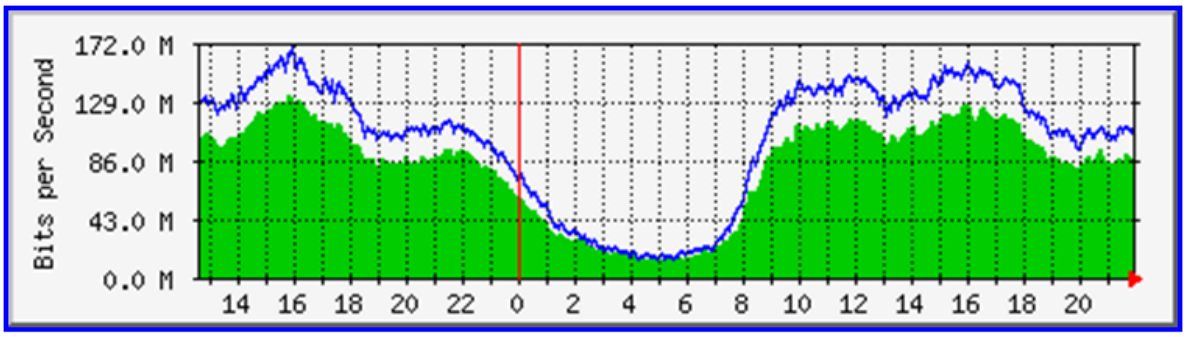
VERDE ### Tráfico entrante al NAP en bits por segundo

AZUL ### Tráfico saliente desde el NAP en bits por segundo

QUITO



GUAYAQUIL



Las gráficas anteriores fueron tomadas el lunes 28 de marzo del 2010 a las 17:39.

5.3 POLÍTICAS DE SEGURIDAD, PEERING Y ENRUTAMIENTO

5.3.1 POLÍTICAS DE SEGURIDAD

Son reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños. Es importante que al momento de formular las políticas de seguridad, se consideren por lo menos los siguientes aspectos:

- Llevar a cabo un análisis de riesgos periódico que permita mantener una adecuada visión de los riesgos de seguridad de la información a los que están expuestos los activos y desarrollar las medidas necesarias para limitar y reducir dichos riesgos.

- Desarrollar una completa normativa de seguridad que regule las condiciones en las que la empresa, dentro del alcance establecido, debe desarrollar su actividad para respetar los requerimientos de seguridad establecidos.

- Destinar los recursos y medios necesarios para desarrollar todas las medidas de seguridad que se determinen, manteniendo un adecuado balance entre coste y beneficio.

- Establecer un plan de formación y concienciación en materia de seguridad de la información que ayude a todo el personal implicado a conocer y cumplir las medidas de seguridad establecidas y a participar de forma proactiva en la gestión de la seguridad de la información.

- Desarrollar todas las medidas necesarias para garantizar la adecuada gestión de los incidentes de seguridad que puedan producirse, y que permitan la resolución tanto de las incidencias menores como de las situaciones que puedan poner en riesgo la continuidad de las actividades contempladas.

- Establecer periódicamente un conjunto de objetivos e indicadores en materia de seguridad de la información que permitan el adecuado seguimiento de la evolución de la seguridad dentro de la empresa.

- Establecer una metodología de revisión, auditoría y mejora continua del sistema, siguiendo un ciclo que garantice el mantenimiento continuo de los niveles de seguridad deseados.

- Impulsar y velar por el desarrollo, cumplimiento y mantenimiento del Plan de Continuidad de Negocio (PCN) de EJIE como máxima responsable del mismo. La Dirección entiende el PCN de EJIE como un proceso de carácter cíclico y continuo, con responsables asignados, y con procedimientos técnicos y organizativos, definidos y auditables.

5.3.2 POLÍTICAS PARA INTERCAMBIO DE TRÁFICO (PEERING) EN NAP.EC

El intercambio de tráfico en NAP.EC es multilateral obligatorio, es decir, cada proveedor conectado intercambia tráfico con todos los demás participantes.

5.3.3 POLÍTICAS SOBRE EL ENRUTAMIENTO

Las siguientes políticas de enrutamiento rigen la operación y administración de NAP.EC:

- Protocolo de enrutamiento BGP.
- Una sola sesión BGP por conexión con un servidor de rutas.
- No se permite ebgp multi-hop.
- Se bloquean redes privadas, redes experimentales o de investigación, redes reservadas por IANA y rutas por defecto.
- Se bloquean prefijos con máscaras de más de 24 bits.
- No se filtran “prefijos válidos”, ni aplicaciones (en ambos extremos de la sesión BGP).
- Se eliminan del ASPATH los ASN privados.

- Desde NAP.EC, "todos" los prefijos son anunciados a todos los proveedores con comunidad no-export.
- En el extremo de NAP.EC, se maneja un máximo para el número de prefijos recibidos por sesión.
- Si el proveedor desea configurar un máximo para el número de prefijos recibidos desde NAP.EC, este número máximo deberá ser consultado y coordinado con la administración de NAP.EC.
- Si el proveedor desea utilizar el enlace interurbano de NAP.EC los prefijos que anuncie en cada nodo deberán ser diferentes.
- Antes de pasar al proceso de selección de rutas, a todos los prefijos recibidos en NAP.EC se les asigna un valor de cero para el atributo MED,
- Luego del proceso de selección de rutas, los prefijos son anunciados por NAP.EC con los siguientes valores del atributo MED: 0 si ha sido recibido en el mismo nodo (ciudad) y 100 si ha sido recibido en otro nodo (ciudad).

CAPÍTULO 6.

SIMULACIÓN DE LA RED

El capítulo 6, está dedicado a la simulación del escenario planteado en la que se verifique la correcta operación de los protocolos (protocolos de enrutamiento y enrutados). Para esto, se utilizará un software que incluye un ambiente gráfico para creación de topología de redes y un emulador de hardware de enrutadores.

El simulador a utilizar para efectos de nuestro estudio y el que mejor se adapto a las necesidades requeridas es el GNS3.

6.1 SOFTWARE DE SIMULACIÓN.

6.1.1 INTRODUCCIÓN

En la actualidad la demanda de las empresas por mejorar sus procesos operativos conlleva en la mayoría de los casos, la instalación de nuevas aplicaciones o la modificación de las aplicaciones existentes, lo que a su vez impacta en el rendimiento de la red corporativa.

Los Administradores de Redes se enfrentan diariamente al desafío de manejar estos cambios y buscar opciones para mejorar los tiempos de respuesta a través de nuevas configuraciones en sus dispositivos de redes como: implementar políticas de calidad de servicio QoS, habilitar protocolos de enrutamiento entre otros. Y todo esto con la presión de no poder probar sus nuevas ideas en horas de trabajo, porque la desconexión de los usuarios de la red no es una opción factible.

¿Entonces qué hacen la mayoría de los Administradores de Redes para implementar los cambios propuestos? Normalmente programan estos operativos en horarios en que los usuarios no están, pasada la jornada laboral o para el fin de semana, con el estrés adicional de que si se presentan inconvenientes o los resultados no son los que esperaban, deben reversar los cambios antes de que regresen los usuarios, enfrentándose en una lucha contra el reloj a cada paso.

6.1.2 GNS3 (SIMULADOR DE RED GRÁFICO)

Es un simulador gráfico de redes que permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos. Hasta el momento GNS3 soporta el IOS de routers, ATM / Frame Relay[23] / Switchs Ethernet y PIX[24] Firewalls.

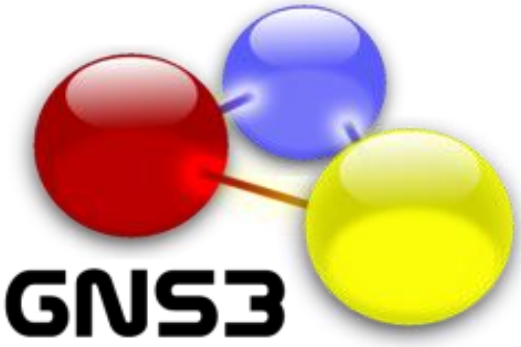


FIGURA 6.34 Logo del software de simulación
Fuente: http://www.gns3.net/

Para permitir completar simulaciones, GNS3 está estrechamente vinculada con:

- Dynamips, es el núcleo del programa que permite emulación de las imágenes IOS de Cisco (1700, 2600, 3600, 3700 y 7200).

- Dynagen, un texto basado en front-end para Dynamips.
  GNS3 también utiliza el formato .INI de configuración e integra la consola de administración que permite a los usuarios listar los dispositivos, suspender y recargar instancias, determinar y administrar los valores de idle-pc, realizar capturas, y mucho mas.

- Pemu, es un servidor de seguridad PIX de Cisco, para salvar las configuraciones.

---

23. Es una técnica de comunicación mediante retransmisión de tramas para redes de circuito virtual

24. Private Internet Exchange para referirse a modelos de equipos Cortafuegos

6.1.3 APLICACIÓN

GNS3 está destinado a complementar la aplicación Dynamips para que al usuario le sea más fácil la instalación, la creación de escenarios y su visualización. Cuando se instala GSN3 se puede observar que las herramientas antes mencionadas (Dynagen, Dynamips y Pemu) quedan instaladas y configuradas.

Solo hará falta la configuración de la imagen IOS, además de su ubicación, para guardar los futuros escenarios.A la hora de crear los escenarios con GNS3 va a resultar más sencillo, ya que sólo habrá que arrastrar los routers que se quieran utilizar e ir cableándolos. Esta manera de trabajar facilitará la conexión entre redes, debido a que tiene instalado un software que permite la configuración de todas las tarjetas Ethernet que se tengan instaladas. Esto permite hacer tantas configuraciones como se desee, ya sean virtuales como reales.

GNS3 facilita los siguientes modos de funcionamiento:

- La construcción de la topología.
- La ejecución y parada de órdenes en las máquinas simuladas.
- La destrucción de la topología.
- La conexión con redes existentes mediante tarjetas Ethernet.
- La posibilidad de salvar configuraciones, tanto de los *routers* como del propio escenario.

6.1.4 UTILIZACIÓN DE RECURSOS

Dynamips hace uso intensivo de memoria RAM y CPU en orden de lograr la magia de la emulación. Si su intención es de ejecutar una imagen de IOS que requiere 256 MB de RAM en un router 7200 real, y dedica 256 MB de RAM a la instancia de su router virtual, este utilizara 256 MB de memoria para funcionar.

Dynamips utiliza por defecto 16 MB en Windows para cache las transacciones JIT. Este será el tamaño total de trabajo; debido a Dynamips archivos para trazar un mapa de la memoria virtual de los routers. En el directorio de trabajo usted hallara archivos temporarios “RAM” cuyo tamaño es igual a la memoria RAM de los routers virtuales. Su sistema operativo cacheara en la RAM las secciones de los archivos nmap que están siendo utilizados.

Dynamips también hace uso intensivo de CPU, porque esta emulando la CPU de un router instrucción-por-instrucción. En principio no tiene manera de saber cuando el router virtual esta en estado ocioso (idle), por esa razón ejecuta diligentemente todas las instrucciones que constituyen las rutinas de idle del IOS, igualmente que las instrucciones que conforman el “real” funcionamiento. Pero una vez que haya ejecutado el proceso de “Idle-PC” para una determinada imagen de IOS, la utilización de CPU decrecerá en forma drástica.

6.1.5 IMÁGENES IOS

Dynamips ejecuta imágenes de Cisco IOS reales. Los cuales se deberá buscar por cuenta propia ya que solo si se es cliente de Cisco puede adquirirla. En Windows, ubicar la imagen en C:\Program Files\Dynamips\images. Puede colocar las imágenes en cualquier ubicación, pero los laboratorios de ejemplo están configurados para buscar en esa locación.

Las imágenes del Cisco IOS están comprimidas. Estas imágenes comprimidas funcionan bien con Dynamips, aunque el proceso de arranque es significativamente mas lento debido a la descompresión (igual que en los routers reales). Es recomendable que descomprima las mismas de antemano así el emulador no tiene que realizar esa tarea.

Unzip –p c7200-g6ik8s-mz.124-2.T1.bin > c7200-g6ik8s-mz.124-2.T1.image

6.2 TOPOLOGÍA DE LA RED SIMULADA

Como se estudió en el Capítulo 5, la topología real de NAP.EC es extensa, por tal razón no se podrá realizar la simulación de todos los routers que lo conforman, el escenario planteado se lo realizará utilizando la herramieta GNS3 (detallada en punto 6.1) en la que se verifique la correcta operación del protocolo BGP con IPv6.

GNS3 al ser utilizado como plataforma de entrenamiento no puede reemplazar al router real y al hacer uso excesivo de los recursos del CPU no es recomendable configurar un gran número de routers, por esta razón al conocer que NAP.EC lo conforman tanto un router en Quito como uno en Guayaquil, hemos configurado seis routers de los cuales los dos primeros representa el NAP (Quito - Guayaquil) y los cuatro siguientes distribuidos de la siguiente forma: dos routers (TE_UNO, TELMEX) para Quito y dos routers para Guayaquil (ECUANET, PORTA). (Ver Figura 6.2).

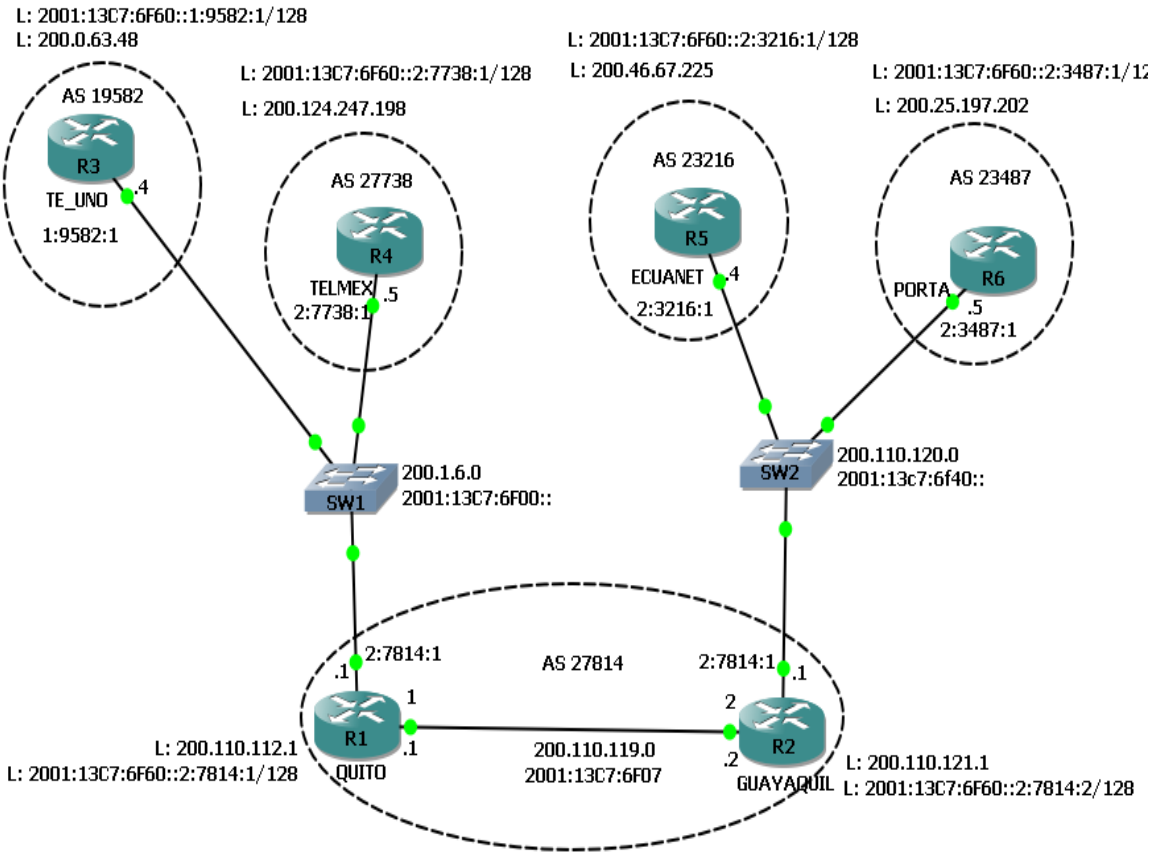


FIGURA 6.35 Topología de la red simulada

6.3 ASIGNACIÓN DE DIRECCIONES IPv6

Las asignaciones deben ser realizadas de acuerdo con las recomendaciones existentes [RFC3177, RIRs on 48][25], las cuales resumimos aquí como:

/48 en el caso general, excepto para suscriptores muy grandes.
/64 cuando se conoce por diseño que una y sólo una subred es necesaria.
/128 cuando se conoce absolutamente que uno y sólo un dispositivo se está conectando.

A los RIRs no les concierne el tamaño de direcciones que los ISPs realmente asignan. Por lo tanto, los RIRs no pedirán información detallada sobre redes de usuarios IPv6 como lo hicieron en IPv4.

6.3.1 ASIGNACIÓN A LA INFRAESTRUCTURA DEL OPERADOR

Una organización (ISP/LIR) puede asignar un /48 por Pop como un servicio de infraestructura de un operador de servicio IPv6. Cada asignación a un PoP es considerada como una asignación sin tener en cuenta el número de usuarios que usen el PoP. Puede obtenerse una asignación separada para operaciones propias del operador.

6.3.2 ASIGNACIONES DIRECTAS A USUARIOS FINALES

LACNIC realizará asignaciones de direcciones IPv6 portables (independientes del proveedor) directas a usuarios finales según las dos políticas detalladas en los ítems 6.3.2.1 y 6.3.2.2, dependiendo si la organización cuenta o no con asignaciones de direcciones IPv4 portables previamente realizadas por LACNIC.

25. http://lacnic.net/sp/politicas/manual5.html

6.3.2.1 ASIGNACIONES DIRECTAS DE DIRECCIONES IPV6 PORTABLES A USUARIOS FINALES CON ASIGNACIONES IPV4 PORTABLES PREVIAS REALIZADAS POR LACNIC

LACNIC asignará bloques de direcciones IPv6 portables directamente a Usuarios Finales si cuentan con asignaciones de direcciones IPv4 portables previamente realizadas por LACNIC.

En caso de anunciar la asignación en el sistema de rutas inter-dominio de Internet, la organización receptora deberá anunciar un único bloque, que agregue toda la asignación de direcciones IPv6 recibida.

Las asignaciones se realizarán en bloques menores o iguales a un /32 pero siempre mayores o iguales a un /48.
Siempre que sea posible, sucesivas asignaciones se realizarían de un bloque de direcciones adyacente, pero sólo si se documenta y justifica convenientemente.

6.3.2.2 ASIGNACIONES DIRECTAS DE DIRECCIONES IPV6 PORTABLES A USUARIOS FINALES SIN ASIGNACIONES IPV4 PORTABLES PREVIAS REALIZADAS POR LACNIC

LACNIC asignará bloques de direcciones IPv6 portables directamente a Usuarios Finales, los cuales deberán cumplir con los siguientes requisitos:

a) No ser un LIR o ISP.
b) En caso de anunciar la asignación en el sistema de rutas inter-dominio de Internet, la organización receptora deberá anunciar un único bloque, que agregue toda la asignación de direcciones IPv6 recibida.
c) Proveer información detallada mostrando como el bloque solicitado será utilizado dentro de tres, seis y doce meses.
d) Entregar planes de direccionamiento por al menos un año, y números de terminales sobre cada subred.

e) Entregar una descripción detallada de la topología de la red.
f) Realizar una descripción detallada de los planes de encaminamiento de la red, incluyendo los protocolos de encaminamiento a ser usados, así también como cualquier limitación existente.

Las asignaciones se realizarán en bloques menores o igual a un /32 pero siempre mayores o iguales a un /48.

Siempre que sea posible, sucesivas asignaciones se realizarían de un bloque de direcciones adyacente, pero sólo si se documenta y justifica convenientemente.

6.3.3 MICROASIGNACIÓN EN IPV6

LACNIC podrá realizar micro-asignaciones en casos de proyectos e infraestructuras de redes claves o críticas para el funcionamiento, y desarrollo de IPv6 en la región como son IXP (Internet Exchange Point), NAP (Network Access Point), RIR, proveedores de DNS, entre otros. Dichas asignaciones se realizarán en prefijos mayores o igual a un /32 pero siempre menores o iguales a un /48.

En el caso de los IXP o NAP para poder solicitar este tipo de asignaciones las organizaciones deberán cumplir los siguientes requisitos:

1) Documentar adecuadamente los siguientes aspectos:

   a) Demostrar a través de sus estatutos su calidad de IXP o NAP. Deberá poseer al menos tres miembros y una política abierta para la asociación de nuevos miembros.
   b) Enviar un diagrama de la estructura de red de la organización.
   c) Documentar el plan de numeración a instrumentar.

2) Proveer un plan de utilización para los próximos tres y seis meses.

En el resto de las solicitudes se estudiarán basados en el análisis de documentación que justifique los aspectos críticos y/o claves del proyecto.

Todas las micro-asignaciones se asignarán de bloques de direcciones específicamente reservados para este tipo de asignaciones. LACNIC hará pública la lista de dichos bloques y las micro-asignaciones realizadas.

La organización que reciba una micro-asignación no podrá realizar sub-asignaciones con estas direcciones IP.

6.3.4 REGISTRO

Cuando una organización que posee una distribución de espacio IPv6, hace asignación de espacios IPv6, debe registrar la información de asignaciones en una base de datos accesible a los RIRs como corresponde (la información registrada por un RIR puede ser cambiada en el futuro por una base de datos para registrar manejo de direcciones).

La información es registrada en unidades de redes /48 asignadas. Cuando a una organización se le cede más de una /48 la organización que la asigna es responsable de asegurar que el espacio de direcciones esté registrado en una base de datos RIR/NIR.

Los RIRs usarán los datos registrados para calcular el HD Ratio en el momento de la solicitud, para subsecuentes distribuciones y para verificar eventuales cambios en las asignaciones.

Los RIRs deben mantener sistemas y prácticas que protejan la seguridad de la información personal y comercial que es usada en la evaluación de solicitudes, pero que no es requerida para registro público.

6.3.5 RESOLUCIÓN INVERSA

Cuando un RIR asigna espacio de direcciones IPv6 a una organización, también está delegando la responsabilidad de manejar la zona de consulta reversa que corresponde al espacio de direcciones IPv6 asignado. Cada organización debe manejar debidamente su zona de consulta reversa. Cuando una organización hace una asignación de direcciones, debe delegar a la organización asignada, bajo pedido, la responsabilidad de manejar la zona de consulta reversa que corresponde a las direcciones asignadas.

6.3.6 POSEEDORES DE IPv6 YA EXISTENTES

Las organizaciones que hayan recibido distribuciones de IPv6 /35 bajo la política previa de IPv6 [RIRv6 Policies] están inmediatamente autorizadas a expandir su distribución a un prefijo de direcciones /32 sin necesidad de justificación. El prefijo de direcciones /32 contendrá el prefijo mayor ya distribuido (uno o múltiples prefijos /35 en muchos casos) que ya ha sido reservado por el RIR para una subsecuente distribución a la organización. Las solicitudes de espacio adicional más allá del mínimo tamaño /32 serán evaluadas como se discutió en otra parte del documento.

6.4 CONFIGURACIONES DEL EQUIPAMIENTO SIMULADO

6.4.1 CONFIGURACIÓN DEL ROUTER 1 (QUITO)

```
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname QUITO // nombre del router
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
enable secret 5 $1$j4lj$Lyr6bPJumoj4riJJOCXqY1
!
```

```
no aaa new-model
ip source-route
ip cef
!
!
ipv6 unicast-routing
ipv6 cef
!
multilink bundle-name authenticated
!
!
!
archive
 log config
  hidekeys
!
!
!
interface Loopback1 \\  Interface de Loopback
 ip address 200.110.112.1 255.255.255.0 \\ Dirección Ipv4
 ipv6 address 2001:13C7:6F60::2:7814:1/128 \\ Dirección Ipv6
 ipv6 nd ra mtu suppress
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface FastEthernet1/0 \\  Interface FastEthernet1/0
 ip address 200.110.119.1 255.255.255.0 \\ Dirección Ipv4
 duplex auto
 speed auto
 ipv6 address 2001:13C7:6F07::1/64 \\ Dirección Ipv6
!
interface FastEthernet1/1 \\  Interface FastEthernet1/1
 ip address 200.1.6.1 255.255.255.0 \\ Dirección Ipv4
 duplex auto
 speed auto
 ipv6 address 2001:13C7:6F00::2:7814:1/64 Dirección Ipv6
!
router bgp 27814\\ Configura el proceso de enrutamiento BGP
 bgp log-neighbor-changes
 neighbor 2001:13C7:6F00::1:9582:1 remote-as 19582 UIO \\ Asocia una descripcion a
un router vecino
 neighbor 2001:13C7:6F00::1:9582:1 description TEUNO_UIO \\ Asocia una descripcion
  a un router vecino
 neighbor 2001:13C7:6F00::2:7738:1 remote-as 27738 \\  Añade una entrada a la
tabla de vecinos BGP
 neighbor 2001:13C7:6F00::2:7738:1 description TELMEX_UIO UIO \\ Asocia una
  descripcion a un router vecino
 neighbor 2001:13C7:6F07::2 remote-as 27814\\  Añade una entrada a la tabla de
vecinos BGP
 neighbor 2001:13C7:6F07::2 description IBGP_CON_GYE
 neighbor 200.1.6.4 remote-as 19582\\  Añade una entrada a la tabla de vecinos BGP
 neighbor 200.1.6.4 description TEUNO_UIO UIO \\ Asocia una descripcion a un router
  vecino
```

```
 neighbor 200.1.6.5 remote-as 27738\\  Añade una entrada a la tabla de vecinos BGP
 neighbor 200.1.6.5 description TELMEX_UIO UIO \\ Asocia una descripcion a un router
  vecino
 neighbor 200.110.119.2 remote-as 27814 \\  Añade una entrada a la tabla de vecinos
BGP
 neighbor 200.110.119.2 description IBGP_CON_GYE \\ Asocia una descripcion a un
router   vecino
 neighbor 200.110.119.2 version 4 \\ Configura el software IOS para que acepte sólo
 una versión BGP
 !
 address-family ipv4
  no neighbor 2001:13C7:6F00::1:9582:1 activate
  no neighbor 2001:13C7:6F00::2:7738:1 activate
  no neighbor 2001:13C7:6F07::2 activate
  neighbor 200.1.6.4 activate
  neighbor 200.1.6.4 send-community \\ Especifica a que vecino BGP le debe enviar un
  atributo de "comunidades"
  neighbor 200.1.6.4 remove-private-as
  neighbor 200.1.6.4 soft-reconfiguration inbound \\ Configura el IOS del software para
  que pueda almacenar actualizaciones
  neighbor 200.1.6.4 prefix-list 10 in \\ Distribuye la información sobre los vecinos BGP
 como se especifica en una lista de prefijos
  neighbor 200.1.6.4 prefix-list 10 out \\ Distribuye la información sobre los vecinos
  BGP   como se especifica en una lista de prefijos
  neighbor 200.1.6.4 route-map ENTRADA_UIO_1 in
  neighbor 200.1.6.4 route-map TODO_UIO out
  neighbor 200.1.6.4 maximum-prefix 2000 80 restart 60
  neighbor 200.1.6.5 activate
  neighbor 200.1.6.5 send-community \\ Especifica a que vecino BGP le debe enviar un
  atributo de "comunidades"
  neighbor 200.1.6.5 remove-private-as
  neighbor 200.1.6.5 soft-reconfiguration inbound \\ Configura el IOS del software   para
  que pueda almacenar actualizaciones
  neighbor 200.1.6.5 prefix-list 10 in \\ Distribuye la información sobre vecinos BGP
 como se especifica en una lista de prefijos
  neighbor 200.1.6.5 prefix-list 10 out \\ Distribuye la información sobre vecinos BGP
 como se especifica en una lista de prefijos
  neighbor 200.1.6.5 route-map ENTRADA_UIO_1 in
  neighbor 200.1.6.5 route-map SOLO_UIO out
  neighbor 200.1.6.5 maximum-prefix 2000 80 restart 60
  neighbor 200.110.119.2 activate
  neighbor 200.110.119.2 send-community \\ Especifica a que vecino BGP le debe
  enviar un   atributo de "comunidades"
  neighbor 200.110.119.2 next-hop-self \\ Desactiva el proceso de próximo salto de las
  actualizaciones BGP en el router
  neighbor 200.110.119.2 soft-reconfiguration inbound \\ Configura el IOS del software
  para   que pueda almacenar actualizaciones
  neighbor 200.110.119.2 maximum-prefix 2000 80 restart 60
  no auto-summary
  no synchronization
  network 200.110.112.0 \\ Especifica la lista de redes en un proceso de enrutamiento
  BGP
 exit-address-family
 !
 address-family ipv6
  neighbor 2001:13C7:6F00::1:9582:1 activate
```

neighbor 2001:13C7:6F00::1:9582:1 send-community \\ Especifica a que vecino BGP le debe enviar un atributo de "comunidades"
neighbor 2001:13C7:6F00::1:9582:1 remove-private-as
neighbor 2001:13C7:6F00::1:9582:1 soft-reconfiguration inbound \\ Configura el IOS del software para que pueda almacenar actualizaciones
neighbor 2001:13C7:6F00::1:9582:1 prefix-list 100 in \\ Distribuye la información sobre vecinos BGP como se especifica en una lista de prefijos
neighbor 2001:13C7:6F00::1:9582:1 prefix-list 100 out \\ Distribuye la información sobre vecinos BGP como se especifica en una lista de prefijos
neighbor 2001:13C7:6F00::1:9582:1 route-map ENTRADA_UIO_1 in
neighbor 2001:13C7:6F00::1:9582:1 route-map TODO_UIO out
neighbor 2001:13C7:6F00::1:9582:1 maximum-prefix 2000 80 restart 60
neighbor 2001:13C7:6F00::2:7738:1 activate
neighbor 2001:13C7:6F00::2:7738:1 send-community both \\ Especifica a que vecino BGP le debe enviar un atributo de "comunidades"
neighbor 2001:13C7:6F00::2:7738:1 remove-private-as
neighbor 2001:13C7:6F00::2:7738:1 soft-reconfiguration inbound \\ Configura el IOS del software para que pueda almacenar actualizaciones
neighbor 2001:13C7:6F00::2:7738:1 prefix-list 100 in \\ Distribuye la información sobre los vecinos BGP como se especifica en una lista de prefijos
neighbor 2001:13C7:6F00::2:7738:1 prefix-list 100 out \\ Distribuye la información sobre los vecinos BGP como se especifica en una lista de prefijos
neighbor 2001:13C7:6F00::2:7738:1 route-map ENTRADA_UIO_1 in
neighbor 2001:13C7:6F00::2:7738:1 route-map SOLO_UIO out
neighbor 2001:13C7:6F00::2:7738:1 maximum-prefix 2000 80 restart 60
neighbor 2001:13C7:6F07::2 activate
neighbor 2001:13C7:6F07::2 send-community both \\ Especifica a que vecino BGP le debe enviar un atributo de "comunidades"
neighbor 2001:13C7:6F07::2 next-hop-self \\ Desactiva el proceso de próximo salto de las actualizaciones BGP en el router
neighbor 2001:13C7:6F07::2 soft-reconfiguration inbound \\ Configura el IOS del software para que pueda almacenar actualizaciones
neighbor 2001:13C7:6F07::2 maximum-prefix 2000 80 restart 60
network 2001:13C7:6F60::2:7814:1/128 \\ Especifica la lista de redes en un proceso de enrutamiento BGP
exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
ip bgp-community new-format \\ Visualiza las comunidades BGP en el formato AA:NN (sistema autónomo – numero de comunidad – numero de 2 bytes)
ip community-list 1 permit 27814:1 \\ Crea una lista de comunidad BGP y controla su acceso
ip community-list 2 permit 27814:2 \\ Crea una lista de comunidad BGP y controla su acceso
ip community-list 10 permit 27814:10 \\ Crea una lista de comunidad BGP y controla su acceso
ip community-list 20 permit 27814:20 \\ Crea una lista de comunidad BGP y controla su acceso
!
!
!
ip prefix-list 10 description Elimina prefijos con mascaras de mas de 24 bits, ruta por defecto y redes privadas

ip prefix-list 10 seq 10 deny 0.0.0.0/0 ge 25 \\ Crea una entrada en una lista de prefijos
ip prefix-list 10 seq 20 deny 0.0.0.0/0 \\ Crea una entrada en una lista de prefijos
ip prefix-list 10 seq 30 deny 10.0.0.0/8 le 32 \\ Crea una entrada en una lista de prefijos
ip prefix-list 10 seq 40 deny 169.254.0.0/16 le 32 \\ Crea una entrada en una lista de prefijos
ip prefix-list 10 seq 50 deny 172.16.0.0/12 le 32 \\ Crea una entrada en una lista de prefijos
ip prefix-list 10 seq 60 deny 192.168.0.0/16 le 32 \\ Crea una entrada en una lista de prefijos
ip prefix-list 10 seq 70 deny 224.0.0.0/8 le 32 \\ Crea una entrada en una lista de prefijos
ip prefix-list 10 seq 100 permit 0.0.0.0/0 le 32 \\ Crea una entrada en una lista de prefijos
logging alarm informational
!
!
ipv6 prefix-list 100 seq 10 deny 2001:DB8::/32 le 128 \\ Crea una entrada en una lista de prefijos ipv6
ipv6 prefix-list 100 seq 20 deny 2002::/16 le 128 \\ Crea una entrada en una lista de prefijos ipv6
ipv6 prefix-list 100 seq 30 deny 2000::/3 ge 31 le 48 \\ Crea una entrada en una lista de prefijosipv6
ipv6 prefix-list 100 seq 40 permit ::/0 le 128\\ Crea una entrada en una lista de prefijos
!
!
!
route-map SALIDA_UIO_C permit 10 \\ Controlan y modifican la informacion de enrutamiento y para definir las condiciones con las que se distribuiran las rutas entre routers
 match ip address prefix-list 30
 set community no-export
!
route-map SALIDA_UIO_C permit 11 \\ Controlan y modifican la informacion de enrutamiento y para definir las condiciones con las que se distribuiran las rutas entre routers
 match ip address prefix-list 31
 set metric 100
 set community no-export
!
route-map SALIDA_UIO_C permit 20\\ Controlan y modifican la informacion de enrutamiento y para definir las condiciones con las que se distribuiran las rutas entre routers
 match community 1
 set community no-export
!
route-map SALIDA_UIO_C permit 30 \\ Controlan y modifican la informacion de enrutamiento y para definir las condiciones con las que se distribuiran las rutas entre routers
 match community 2
 set metric 100
 set community no-export
!
route-map SOLO_UIO permit 10 \\ Controlan y modifican la informacion de enrutamiento y para definir las condiciones con las que se distribuiran las rutas entre routers

```
match ip address prefix-list 30
set community no-export
!
route-map SOLO_UIO permit 20 \\ Controlan y modifican la informacion de enrutamiento y para definir las condiciones con las que se distribuiran las rutas entre routers
 match community 1
 set community no-export
!
route-map SOLO_UIO permit 30 \\ Controlan y modifican la informacion de enrutamiento y para definir las condiciones con las que se distribuiran las rutas entre routers
 match community 20
 set metric 100
 set community no-export
!
route-map ENTRADA_UIO_2 permit 10 \\ Controlan y modifican la informacion de enrutamiento y para definir las condiciones con las que se distribuiran las rutas entre routers
 set community 27814:1 27814:10
!
route-map ENTRADA_UIO_1 permit 10 \\ Controlan y modifican la informacion de enrutamiento y para definir las condiciones con las que se distribuiran las rutas entre routers
 set metric 0
 set community 27814:1
!
route-map GGC permit 10 \\ Controlan y modifican la informacion de enrutamiento y para definir las condiciones con las que se distribuiran las rutas entre routers
 match ip address prefix-list 40
 set community no-export
!
route-map GGC permit 20 \\ Controlan y modifican la informacion de enrutamiento y para definir las condiciones con las que se distribuiran las rutas entre routers
match as-path 20
 match community 1
 set community no-export
!
route-map GGC permit 30 \\ Controlan y modifican la informacion de enrutamiento y para definir las condiciones con las que se distribuiran las rutas entre routers
 match as-path 30
 match community 20
 set community no-export
!
control-plane
!
gatekeeper
 shutdown
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password cisco
 login
```

6.4.2 CONFIGURACIÓN DEL ROUTER 2 (GUAYAQUIL)

```
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname GUAYAQUIL \\  Nombre del router
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
enable secret 5 $1$5o5D$lgAgOdJl1eO.89CzvEU920
!
no aaa new-model
ip source-route
ip cef
!
!
!
!
ipv6 unicast-routing
ipv6 cef
!
multilink bundle-name authenticated
!
!
!
archive
 log config
  hidekeys
!
!
!
interface Loopback2
 ip address 200.110.121.1 255.255.255.0 \\ Dirección Ipv4
 ipv6 address 2001:13C7:6F60::2:7814:2/128 \\ Dirección Ipv6
 ipv6 nd ra mtu suppress
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface FastEthernet1/0
 ip address 200.110.119.2 255.255.255.0 \\ Dirección Ipv4
 duplex auto
 speed auto
 ipv6 address 2001:13C7:6F07::2/64 \\ Dirección Ipv6
!
interface FastEthernet1/1
 ip address 200.110.120.1 255.255.255.0 \\ Dirección Ipv4
 duplex auto
```

```
 speed auto
 ipv6 address 2001:13C7:6F40::2:7814:1/64
!
router bgp 27814 \\ Configura el proceso de enrutamiento BGP
 no synchronization
 bgp log-neighbor-changes
 network 200.110.121.0 \\ Especifica la lista de redes en un proceso  de enrutamiento
  BGP
 neighbor 2001:13C7:6F07::1 remote-as 27814 \\ Añade una entrada a la tabla de
vecinos BGP
 neighbor 2001:13C7:6F07::1 description IBGP_CON_GYE \\ Asocia una descripcion con
un vecino
 no neighbor 2001:13C7:6F07::1 activate
 neighbor 2001:13C7:6F40::2:3216:1 remote-as 23216 \\ Añade una entrada a la tabla
de vecinos BGP
 neighbor 2001:13C7:6F40::2:3216:1 description ECUANET_GYE \\ Asocia una
descripcion con un vecino
 no neighbor 2001:13C7:6F40::2:3216:1 activate
 neighbor 2001:13C7:6F40::2:3487:1 remote-as 23487 \\ Añade una entrada a la tabla
de vecinos BGP
 neighbor 2001:13C7:6F40::2:3487:1 description PORTA_GYE \\ Asocia una descripcion
con un vecino
 no neighbor 2001:13C7:6F40::2:3487:1 activate
 neighbor 200.110.119.1 remote-as 27814 \\ Añade una entrada a la tabla de vecinos
BGP
 neighbor 200.110.119.1 description IBGP_CON_UIO \\ Asocia una descripcion con un
vecino
 neighbor 200.110.119.1 version 4
 neighbor 200.110.119.1 next-hop-self \\ Desactiva el proceso de próximo salto  de las
actualizaciones BGP del router
 neighbor 200.110.119.1 send-community both  \\ Especifica a que vecino BGP le debe
  enviar un  atributo de "comunidades"
 neighbor 200.110.119.1 soft-reconfiguration inbound \\ Configura el IOS del software
  para  que pueda almacenar actualizaciones
 neighbor 200.110.119.1 maximum-prefix 2000 80 restart 60
 neighbor 200.110.120.4 remote-as 23216\\ Añade una entrada a la tabla de vecinos
BGP
 neighbor 200.110.120.4 description ECUANET_GYE \\ Asocia una descripcion con un
vecino
 neighbor 200.110.120.4 send-community both  \\ Especifica a que vecino BGP le debe
  enviar un  atributo de "comunidades"
 neighbor 200.110.120.4 remove-private-as
 neighbor 200.110.120.4 soft-reconfiguration inbound \\ Configura el IOS del software
  para  que pueda almacenar actualizaciones
 neighbor 200.110.120.4 prefix-list 10 in \\Distribuye información sobre los vecinos BGP
como se especifica en una lista de prefijos
 neighbor 200.110.120.4 prefix-list 10 out \\Distribuye información sobre los vecinos
BGP como se especifica en una lista de prefijos
 neighbor 200.110.120.4 route-map ENTRADA_GYE_1 in
 neighbor 200.110.120.4 route-map TODO_GYE out
 neighbor 200.110.120.4 maximum-prefix 2000 80 restart 60
 neighbor 200.110.120.5 remote-as 23487\\ Añade una entrada a la tabla de vecinos
BGP
 neighbor 200.110.120.5 description PORTA_GYE \\ Asocia una descripcion con un
vecino
 neighbor 200.110.120.5 send-community both \\ Especifica a que vecino BGP le debe
```

```
 enviar un  atributo de "comunidades"
 neighbor 200.110.120.5 remove-private-as
 neighbor 200.110.120.5 soft-reconfiguration inbound \\ Configura el IOS del software
  para  que pueda almacenar actualizaciones
 neighbor 200.110.120.5 prefix-list 10 in \\Distribuye información sobre los vecinos BGP
como se especifica en una lista de prefijos
 neighbor 200.110.120.5 prefix-list 10 out \\Distribuye información sobre los vecinos
BGP como se especifica en una lista de prefijos
 neighbor 200.110.120.5 route-map ENTRADA_GYE_1 in
 neighbor 200.110.120.5 route-map SOLO_GYE out
 neighbor 200.110.120.5 maximum-prefix 2000 80 restart 60
 no auto-summary
 !
 address-family ipv6
  neighbor 2001:13C7:6F07::1 activate
  neighbor 2001:13C7:6F07::1 send-community both  \\ Especifica a que vecino BGP le
  debe  enviar un  atributo de "comunidades"
  neighbor 2001:13C7:6F07::1 next-hop-self
  neighbor 2001:13C7:6F07::1 soft-reconfiguration inbound \\ Configura el IOS del
  software  para  que pueda almacenar actualizaciones
  neighbor 2001:13C7:6F07::1 maximum-prefix 2000 80 restart 60
  neighbor 2001:13C7:6F40::2:3216:1 activate
  neighbor 2001:13C7:6F40::2:3216:1 send-community both  \\ Especifica a que
  vecino BGP le debe  enviar un  atributo de "comunidades"
  neighbor 2001:13C7:6F40::2:3216:1 remove-private-as
  neighbor 2001:13C7:6F40::2:3216:1 soft-reconfiguration inbound \\ Configura el IOS
  del software  para  que pueda almacenar actualizaciones
  neighbor 2001:13C7:6F40::2:3216:1 prefix-list 100 in \\ Distribuye información sobre
 los vecinos BGP como se especifica en una lista de prefijos
  neighbor 2001:13C7:6F40::2:3216:1 prefix-list 100 out \\ Distribuye información
sobre los vecinos BGP como se especifica en una lista de prefijos

  neighbor 2001:13C7:6F40::2:3216:1 route-map ENTRADA_GYE_1 in
  neighbor 2001:13C7:6F40::2:3216:1 route-map TODO_GYE out
  neighbor 2001:13C7:6F40::2:3216:1 maximum-prefix 2000 80 restart 60
  neighbor 2001:13C7:6F40::2:3487:1 activate
  neighbor 2001:13C7:6F40::2:3487:1 send-community both  \\ Especifica a que vecino
  BGP le debe  enviar un  atributo de "comunidades"
  neighbor 2001:13C7:6F40::2:3487:1 remove-private-as
  neighbor 2001:13C7:6F40::2:3487:1 soft-reconfiguration inbound\\ Configura el IOS
  del software  para  que pueda almacenar actualizaciones
  neighbor 2001:13C7:6F40::2:3487:1 prefix-list 100 in \\Distribuye información sobre
 los vecinos BGP como se especifica en una lista de prefijos
  neighbor 2001:13C7:6F40::2:3487:1 prefix-list 100 out \\Distribuye información - --
 sobre los vecinos BGP como se especifica en una lista de prefijos
  neighbor 2001:13C7:6F40::2:3487:1 route-map ENTRADA_GYE_1 in \\ controla y
  modifica la informacion de enrutamiento
  neighbor 2001:13C7:6F40::2:3487:1 route-map SOLO_GYE out
  neighbor 2001:13C7:6F40::2:3487:1 maximum-prefix 2000 80 restart 60
  network 2001:13C7:6F60::2:7814:2/128 \\ Especifica la lista de redes en un proceso
de enrutamiento BGP
 exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
```

```
!
ip bgp-community new-format
ip bgp-community new-format \\ Visualiza las comunidades BGP en el formato AA:NN (sistema autónomo – numero de comunidad – numero de 2 bytes)
ip community-list 1 permit 27814:1 \\ Crea una lista de comunidad BGP y controla su acceso
ip community-list 2 permit 27814:2 \\ Crea una lista de comunidad BGP y controla su acceso
ip community-list 10 permit 27814:10 \\ Crea una lista de comunidad BGP y controla su acceso
ip community-list 20 permit 27814:20 \\ Crea una lista de comunidad BGP y controla su acceso
!
!
!
ip prefix-list 10 description Elimina prefijos con mascaras de mas de 24 bits, ruta por defecto y redes privadas
ip prefix-list 10 seq 10 deny 0.0.0.0/0 ge 25 \\  Distribuye información sobre los vecinos BGP como se especifica en una lista de prefijos
ip prefix-list 10 seq 20 deny 0.0.0.0/0 \\  Distribuye información sobre los vecinos BGP como se especifica en una lista de prefijos
ip prefix-list 10 seq 30 deny 10.0.0.0/8 le 32 \\  Distribuye información sobre los vecinos BGP como se especifica en una lista de prefijos
ip prefix-list 10 seq 40 deny 169.254.0.0/16 le 32 \\  Distribuye información sobre los vecinos BGP como se especifica en una lista de prefijos
ip prefix-list 10 seq 50 deny 172.16.0.0/12 le 32 \\  Distribuye información sobre los vecinos BGP como se especifica en una lista de prefijos
ip prefix-list 10 seq 60 deny 192.168.0.0/16 le 32 \\  Distribuye información sobre los vecinos BGP como se especifica en una lista de prefijos
ip prefix-list 10 seq 70 deny 224.0.0.0/8 le 32 \\  Distribuye información sobre los vecinos BGP como se especifica en una lista de prefijos
ip prefix-list 10 seq 80 permit 0.0.0.0/0 le 32 \\  Distribuye información sobre los vecinos BGP como se especifica en una lista de prefijos
logging alarm informational
!
!
ipv6 prefix-list 100 seq 10 deny 2001:DB8::/32 le 128 \\  Distribuye información sobre los vecinos BGP como se especifica en una lista de prefijos ipv6
ipv6 prefix-list 100 seq 20 deny 2002::/16 le 128 \\  Distribuye información sobre los vecinos BGP como se especifica en una lista de prefijos ipv6
ipv6 prefix-list 100 seq 30 deny 2000::/3 ge 31 le 48 \\  Distribuye información sobre los vecinos BGP como se especifica en una lista de prefijos ipv6
ipv6 prefix-list 100 seq 40 permit ::/0 le 128 \\  Distribuye información sobre los vecinos BGP como se especifica en una lista de prefijos ipv6
!
!
route-map SALIDA_GYE_C permit 10 \\ Controlan y modifican la informacion de enrutamiento
 match ip address prefix-list 30
 set community no-export
!
route-map SALIDA_GYE_C permit 11 \\ Controlan y modifican la informacion de enrutamiento
 match ip address prefix-list 31
set metric 100
 set community no-export
```

```
!
route-map SALIDA_GYE_C permit 20 \\ Controlan y modifican la informacion de
enrutamiento
 match community 2
 set community no-export
!
route-map SALIDA_GYE_C permit 30 \\ Controlan y modifican la informacion de
enrutamiento
 match community 1
 set metric 100
 set community no-export
!
route-map SOLO_GYE permit 10 \\ Controlan y modifican la informacion de
enrutamiento
 match ip address prefix-list 30
 set community no-export
!
route-map SOLO_GYE permit 20 \\ Controlan y modifican la informacion de
enrutamiento
 match community 2
 set community no-export
!
route-map SOLO_GYE permit 30 \\ Controlan y modifican la informacion de
enrutamiento
 match community 10
 set metric 100
set community no-export
!
route-map ENTRADA_GYE_2 permit 10 \\ Controlan y modifican la informacion de
enrutamiento
 set community 27814:2 27814:20
!
route-map ENTRADA_GYE_1 permit 10 \\ Controlan y modifican la informacion de
enrutamiento
 set metric 0
 set community 27814:2!
!
!
!
control-plane
!
!
!
gatekeeper
 shutdown
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password cisco
 login
!
end
```

6.4.3 CONFIGURACIÓN DEL ROUTER 3 (TE UNO)

```
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname TEUNO \\ nombre del router
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
enable secret 5 $1$N/U/$82DdUhW6khJV9hIJw8YO80
!
no aaa new-model
ip source-route
ip cef
!
!
!
!
ipv6 unicast-routing
ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
archive
 log config
  hidekeys
!
!
!
!
interface Loopback3
 ip address 200.0.63.48 255.255.255.0
 ipv6 address 2001:13C7:6F60::1:9582:1/128
 ipv6 nd ra mtu suppress
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface FastEthernet1/0
 ip address 200.1.6.4 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2001:13C7:6F00::1:9582:1/64
!
```

```
interface FastEthernet1/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
router bgp 19582 \\ Configura el proceso de enrutamiento BGP
 bgp log-neighbor-changes
 neighbor 2001:13C7:6F00::2:7814:1 remote-as 27814 \\ Añade una entrada a la tabla
de vecinos BGP
 neighbor 200.1.6.1 remote-as 27814  \\ Añade una entrada a la tabla de vecinos BGP
 neighbor 200.1.6.1 description UIO_TEUNO \\ Asocia una descripcion con un vecino
 neighbor 200.1.6.1 version 4 \\  Configura el IOS de Cisco para que acepte una sola
version BGP
 !
 address-family ipv4
  no neighbor 2001:13C7:6F00::2:7814:1 activate
  neighbor 200.1.6.1 activate
  no auto-summary
  no synchronization
  network 200.0.63.0
 exit-address-family
 !
 address-family ipv6
  neighbor 2001:13C7:6F00::2:7814:1 activate
  neighbor 2001:13C7:6F00::2:7814:1 send-community both
  neighbor 2001:13C7:6F00::2:7814:1 soft-reconfiguration inbound
  network 2001:13C7:6F60::1:9582:1/128
 exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
logging alarm informational
!
!
!
control-plane
!
!
!
gatekeeper
 shutdown
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password cisco
 login
!
```

```
end
```

6.4.4 CONFIGURACIÓN DEL ROUTER 4 (TELMEX)

```
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname TELMEX
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
enable secret 5 $1$Dz2S$2Kpw30Nn4uNdU0lRQfMxW/
!
no aaa new-model
ip source-route
ip cef
!
!
!
!
ipv6 unicast-routing
ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
archive
 log config
  hidekeys
!
!
!
interface Loopback4
 ip address 200.124.247.198 255.255.255.0
 ipv6 address 2001:13C7:6F60::2:7738:1/128
 ipv6 nd ra mtu suppress
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface FastEthernet1/0
 ip address 200.1.6.5 255.255.255.0
 duplex auto
```

```
 speed auto
 ipv6 address 2001:13C7:6F00::2:7738:1/64
!
interface FastEthernet1/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
router bgp 27738 \\ Configura el proceso de enrutamiento BGP
 no synchronization
 bgp log-neighbor-changes
 network 200.124.247.0 \\ Especifica las redes en un proceso de enrutamiento BGP
 neighbor 2001:13C7:6F00::2:7814:1 remote-as 27814 \\ Añade una entrada a la tabla
de vecinos BGP
 neighbor 2001:13C7:6F00::2:7814:1 description UIO_TELMEX
 no neighbor 2001:13C7:6F00::2:7814:1 activate
 neighbor 200.1.6.1 remote-as 27814 \\ Añade una entrada a la tabla de vecinos BGP
 neighbor 200.1.6.1 description UIO_TELMEX \\ añade una entrada a la tabla de vecinos
BGP
 neighbor 200.1.6.1 version 4
 no auto-summary
 !
 address-family ipv6
  neighbor 2001:13C7:6F00::2:7814:1 activate
  neighbor 2001:13C7:6F00::2:7814:1 send-community both
  neighbor 2001:13C7:6F00::2:7814:1 soft-reconfiguration inbound
  network 2001:13C7:6F60::2:7738:1/128
 exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
logging alarm informational
!
!
!
control-plane
!
!
!
gatekeeper
 shutdown
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password cisco
 login
!
```

```
end
```

6.4.5 CONFIGURACIÓN DEL ROUTER 5 (ECUANET)

```
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ECUANET \\ Nombre del router
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
enable secret 5 $1$7Evb$KVqkYr/gZiOSal3weJG9u.
!
no aaa new-model
ip source-route
ip cef
!
!
!
!
ipv6 unicast-routing
ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
archive
 log config
  hidekeys
!
!
!
interface Loopback5
 ip address 200.46.67.225 255.255.255.0
 ipv6 address 2001:13C7:6F60::2:3216:1/128
 ipv6 nd ra mtu suppress
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface FastEthernet1/0
 ip address 200.110.120.4 255.255.255.0
 duplex auto
```

```
 speed auto
 ipv6 address 2001:13C7:6F40::2:3216:1/64
!
interface FastEthernet1/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
router bgp 23216 \\
 no synchronization
 bgp log-neighbor-changes
 network 200.46.67.0 \\ Especifica la lista de redes en un proceso de enrutamiento BGP
 neighbor 2001:13C7:6F40::2:7814:1 remote-as 27814 \\ Añade una entrada  a la tabla de vecinos BGP
 neighbor 2001:13C7:6F40::2:7814:1 description ECUANET_GYE \\ Asocia una descripción con un vecino
 no neighbor 2001:13C7:6F40::2:7814:1 activate
 neighbor 200.110.120.1 remote-as 27814 \\ Añade una entrada  a la tabla de vecinos BGP
 neighbor 200.110.120.1 description ECUANET_GYE description ECUANET_GYE \\ Asocia una descripción con un vecino
 neighbor 200.110.120.1 version 4 \\ Configura el IOS de Cisco para que acepte una sola version BGP
 no auto-summary
 !
 address-family ipv6
  neighbor 2001:13C7:6F40::2:7814:1 activate
  neighbor 2001:13C7:6F40::2:7814:1 send-community \\  especifica a que vecino BGP se le debe enviar un atributo "comunidad"
  neighbor 2001:13C7:6F40::2:7814:1 soft-reconfiguration inbound \\ Configura el IOS de Cisco parq ue pueda almacenar actualizaciones
  network 2001:13C7:6F60::2:3216:1/128 \\ Especifica la lista de redes en un proceso de enrutamiento BGP
 exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
logging alarm informational
!
!
!
control-plane
!
!
!
gatekeeper
 shutdown
!
!
line con 0
 stopbits 1
```

```
line aux 0
 stopbits 1
line vty 0 4
 password cisco
 login
!
end
```

6.4.6 CONFIGURACIÓN DEL ROUTER 6 (PORTA)

```
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PORTA \\ Nombre del router
!
boot-start-marker
boot-end-marker
logging message-counter syslog
enable secret 5 $1$T9vM$Tl3fCwxf86gpUSazvosQm0
!
no aaa new-model
ip source-route
ip cef
!
!
!
ipv6 unicast-routing
ipv6 cef
!
multilink bundle-name authenticated
!
!
!
archive
 log config
  hidekeys
!
!
!
interface Loopback5
 no ip address
 ipv6 address 2001:13C7:6F60::2:3487:1/128
 ipv6 nd ra mtu suppress
!
interface Loopback6
 ip address 200.25.197.202 255.255.255.0
!
interface FastEthernet0/0
 no ip address
```

```
 shutdown
 duplex half
!
interface FastEthernet1/0
 ip address 200.110.120.5 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2001:13C7:6F40::2:3487:1/64
!
interface FastEthernet1/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
router bgp 23487
 no synchronization
 bgp log-neighbor-changes
 network 200.25.197.0
 neighbor 2001:13C7:6F40::2:7814:1 remote-as 27814
 neighbor 2001:13C7:6F40::2:7814:1 description PORTA_GYE \\ Asocia una descripción
con un vecino
 no neighbor 2001:13C7:6F40::2:7814:1 activate
 neighbor 200.110.120.1 remote-as 27814 \\ Añade una entrada  a la tabla de vecinos
BGP
 neighbor 200.110.120.1 description PORTA_GYE \\ Asocia una descripción con un
vecino
 neighbor 200.110.120.1 version 4 \\ Configura el IOS de Cisco para que acepte una
sola version BGP
 no auto-summary
 !
 address-family ipv6
  neighbor 2001:13C7:6F40::2:7814:1 activate
  neighbor 2001:13C7:6F40::2:7814:1 send-community \\  especifica a que vecino BGP
se le debe enviar un atributo "comunidad"
  neighbor 2001:13C7:6F40::2:7814:1 soft-reconfiguration inbound \\ Configura el IOS
de Cisco parq ue pueda almacenar actualizaciones
  network 2001:13C7:6F60::2:3487:1/128 \\ Especifica la lista de redes en un proceso
de enrutamiento BGP
 exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
logging alarm informational
!
!
!
control-plane
!
!
!
gatekeeper
```

```
 shutdown
!
!
!
!
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password cisco
 login
!
i
!
!
!
!
end
```

6.5 COMPROBACIÓN DE LA OPERACIÓN DEL PROTOCOLO DE ENRUTAMIENTO Y DEL CUMPLIMIENTO DE POLÍTICAS

6.5.1 COMPROBACIÓN DEL PROTOCOLO DE ENRUTAMIENTO.

En este apartado se van a ver los pasos necesarios para la configuración de BGP y una serie de comandos prácticos de configuración.

- show ip bgp summary
- show bgp ipv6 unicast summary
- show ip route
- show ipv6 route
- show ipv6 prefix-list

Además, se va a tratar otro aspecto importante en la configuración como es el cumplimiento de cada una de las Políticas de Seguridad que tiene Aeprovi, las cuales las vimos más detalladamente en el capítulo 5. Las comprobaciones se las realiza utilizando los siguientes comandos:

6.5.2 CUMPLIMIENTO DE POLÍTICAS.

a) Protocolo de enrutamiento BGP (IPv4 – IPv6)

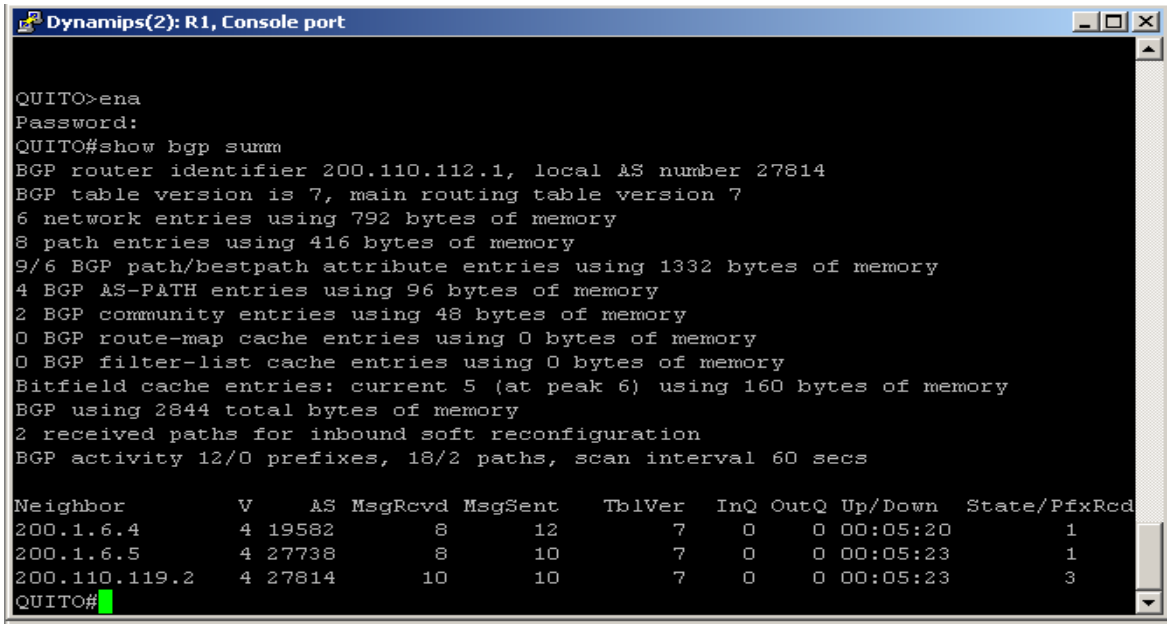


FIGURA 6.36 Protocolo de enrutamiento BGP

IPv6

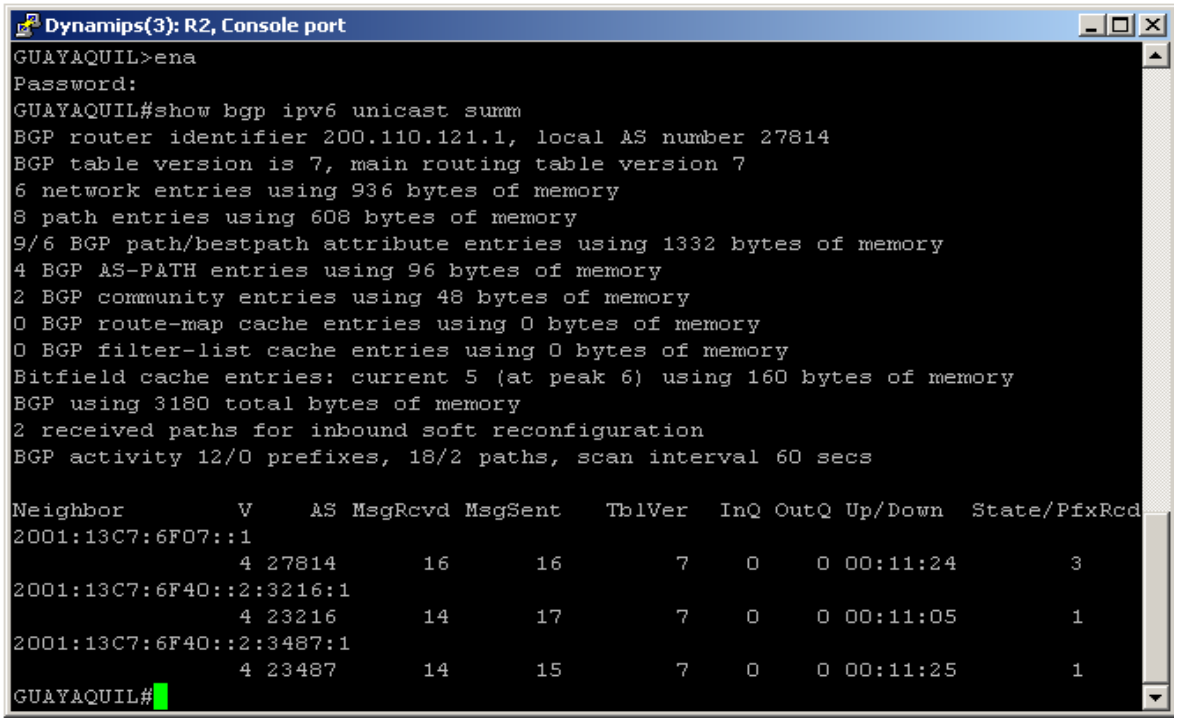


FIGURA 6.37 IPv6

b) Una sola sesión BGP por conexión con un servidos de rutas (IPv4 – IPv6).

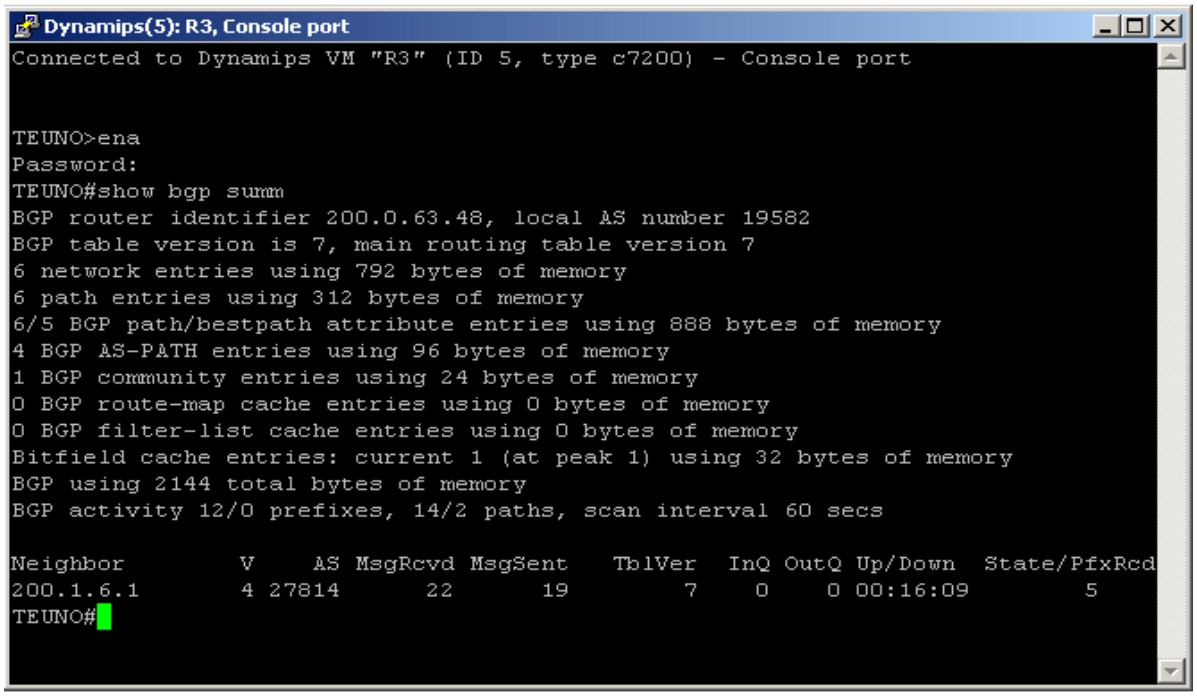


FIGURA 6.38 Sesión BGP

IPv6

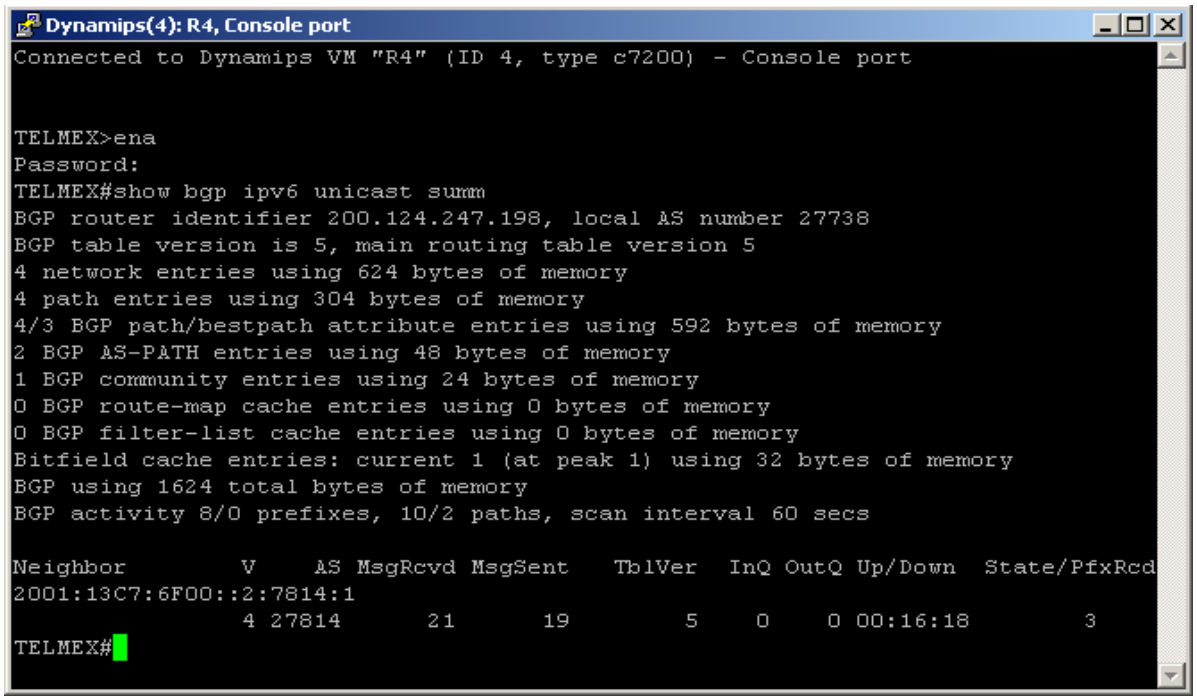


FIGURA 6.39 IPv6

c) Se bloquean redes privadas, redes experimentales o de investigación, redes reservadas por el IANA y rutas por defecto (IPv4 – IPv6).

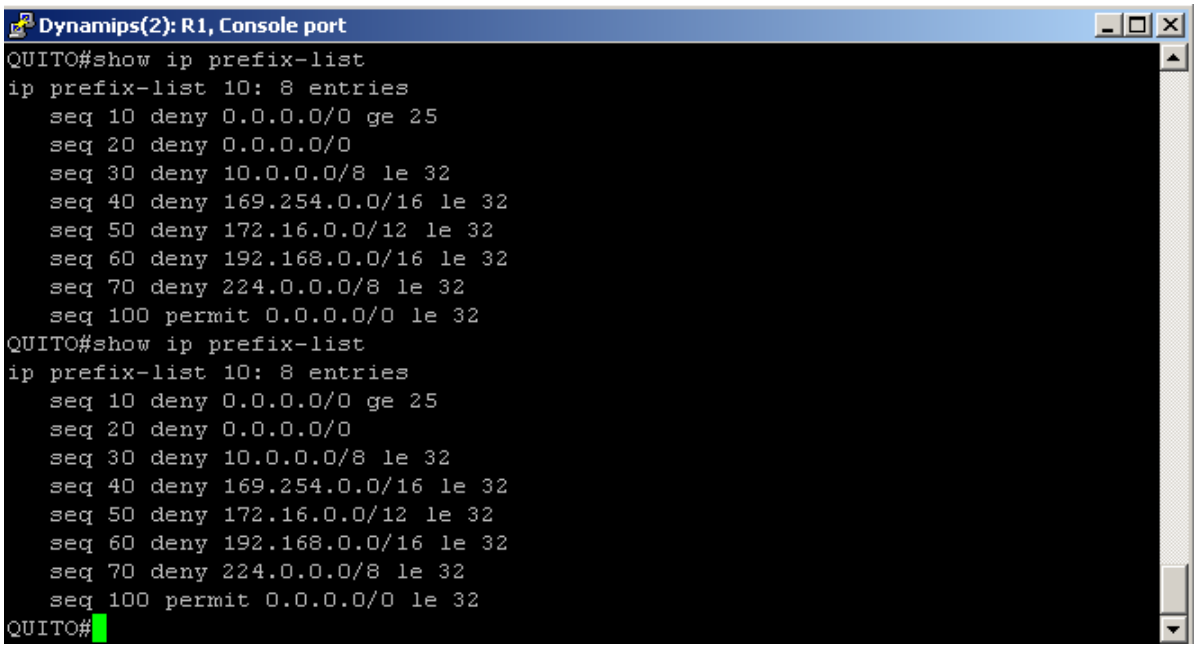


FIGURA 6.40 Bloqueo de Redes privadas y experimentales

IPv6

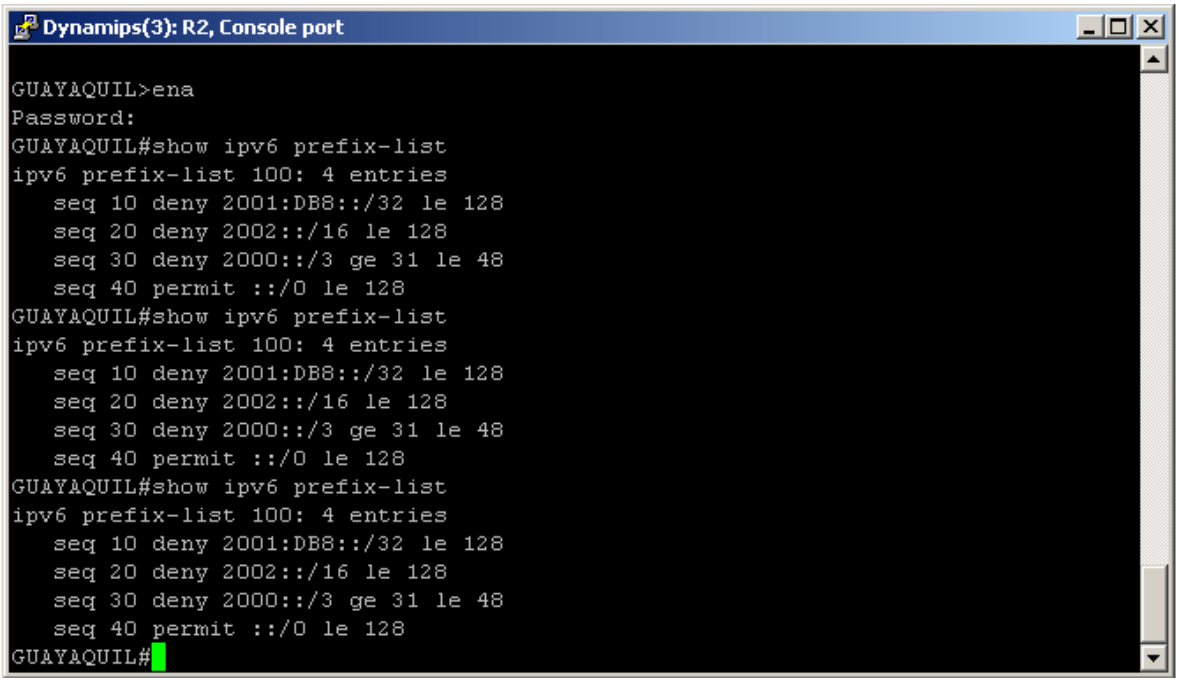


FIGURA 6.41 IPv6

d) Se bloquean prefijos con máscaras de más de 24 bits

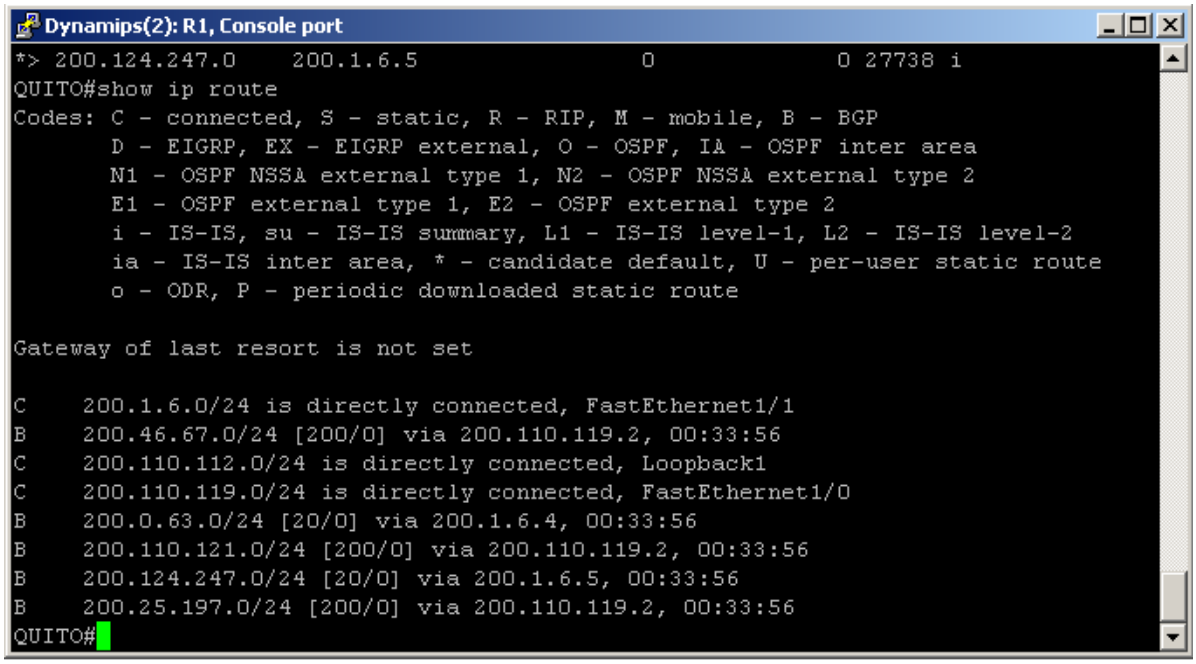


FIGURA 6.42 Bloqueo de prefijos com máscara de más de 24 bits

IPv6

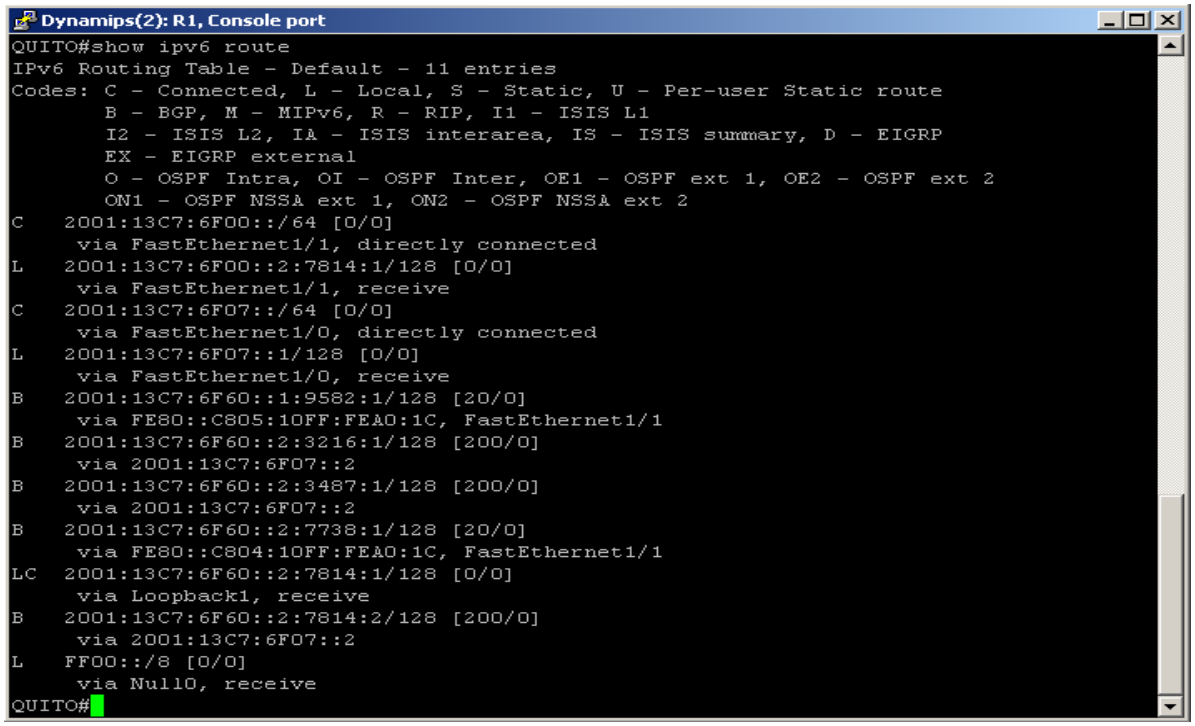


FIGURA 6.43 IPv6

e) Luego del proceso de selección de rutas, los prefijos son anunciados por NAP.EC con los siguientes valores del atributo MED: 0 si ha sido recibido en el mismo nodo (ciudad) y 100 si ha sido recibido en otro nodo (ciudad).

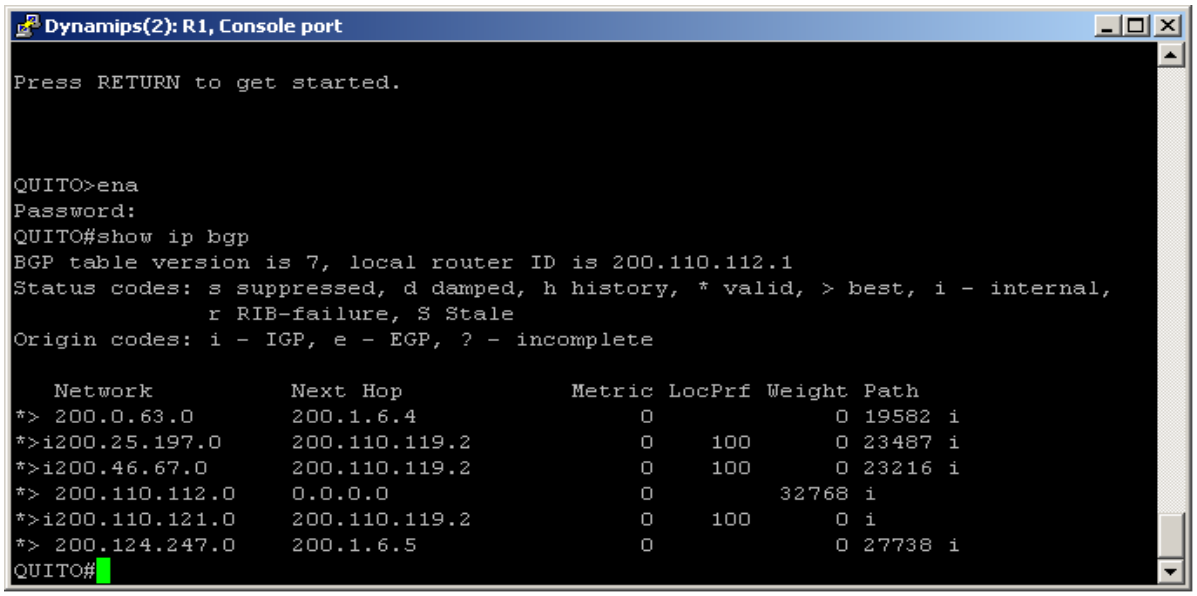


FIGURA 6.44 Verificación del Atributo MED

IPv6

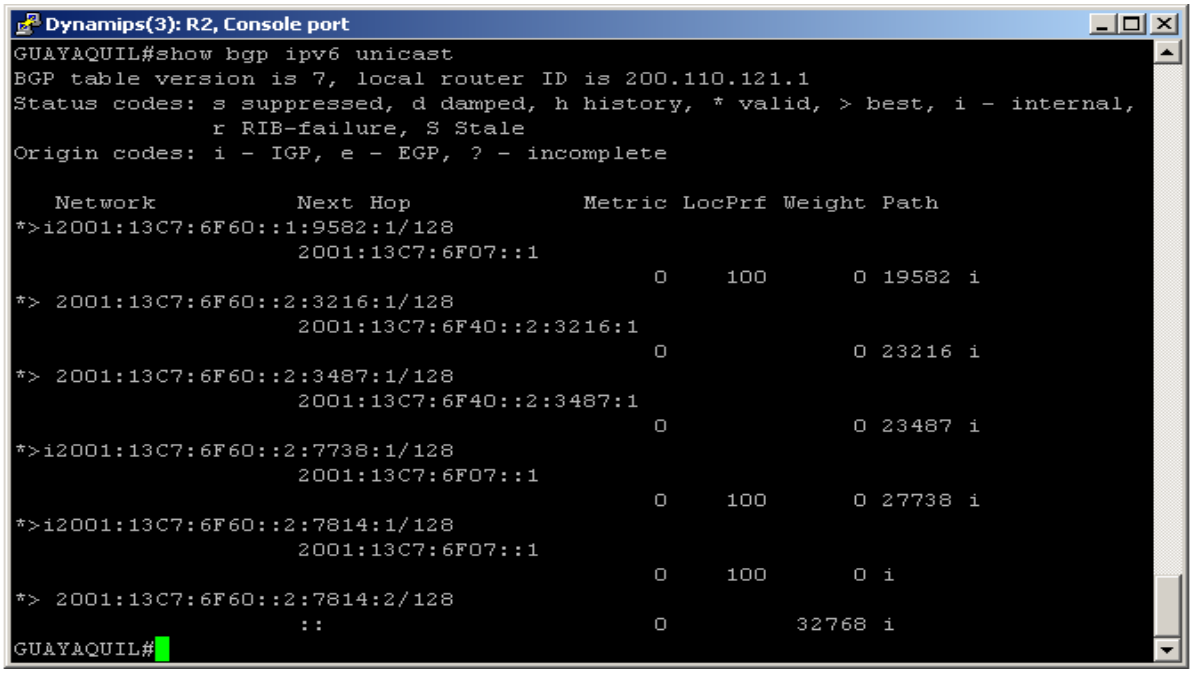


FIGURA 6.45 IPv6

CAPÍTULO 7.

ANÁLISIS ECONÓMICO DE LOS REQUERIMIENTOS TÉCNICOS

En este capítulo, se detalla un análisis costo - beneficio del proyecto, puesto que no solo es importante el estudio técnico sino también determinar la viabilidad económica que este puede representar, para ello se ha basado en el análisis de costos de los equipos, el costo de la implementación, la inversión que representa y concluir determinando también un tiempo estimado en el que se recuperará la inversión de dicha transición en caso de ser implementado.

7.1 REQUERIMIENTOS DE HARDWARE Y SOFTWARE

7.1.1 REQUERIMIENTOS DE HARDWARE

Los equipos que se utilizan son los siguientes:

- Switch Cisco Catalyst 3560G-24TS
- Router Cisco 7200VXR

7.1.1.1 SWITCH CISCO CATALYST 3560G-24TS

Información General:

Tipo de Producto: Conmutador Ethernet
Fabricante: Cisco Systems
Modelo de Producto: Conmutador Gigabit Ethernet Catalyst 3560
Interfaces/Puertos: 24 x 10/100/1000Mbps, 4 puertos Gigabit ethernet SFP (puertos de fibra óptica)
Detalles de Interfaces/Puertos:
• 24 x RJ-45 10/100/1000Base-T Auto-sensing/Auto-negotiating/MDI/MDI-X LAN
• 1 x RJ-45 Consola Gestión
Memoria DRAM: 128MB
Memoria Flash: 32MB
Transferencia de Datos:

- 10Mbps Ethernet Half/Full-duplex
- 100Mbps Fast Ethernet Half/Full-duplex

- 1Gbps Ethernet Gigabit Half/Full-duplex

Tipo de Conexión:

- Categoría 3 UTP 10Base-T
- Categoría 4 UTP 10Base-T
- Categoría 5 UTP 10/100/1000Base-T

Protocolos: RIP, WCCP, LACP, DHCP, DTP, RSTP, OSPF, IGRP, EIGRP, BGP v4, DVMRP, STP, TCP/IP, TFTP, SNMP, Telnet.

Descripción de la Alimentación:
Frecuencia: 50 Hz o 60 Hz
Corriente de entrada: 1,5 Aa 3 A
Consumo de Corriente: 100 W Máx.

7.1.1.2 ROUTER CISCO 7206VXR

Soporta enrutamiento multiprotocolo, capacidades Gigabit para mejorar la integración de datos, voz y video en ambientes, tanto empresariales como de proveedores de servicios sobre una amplia variedad de tipos de interfaces ya sean LAN o WAN. Además este tipo de routers brindan soporte IPv6.

Información General:

Descripción del producto Cisco: 7206VXR - encaminador
Tipo de dispositivo: Encaminador
Procesador: 1 x Broadcom BCM1250 700 MHz
Memoria RAM: 1 GB - SDRAM
Memoria Flash: 64 MB
Puertos: 3 puertos 10/100/1000Mbps o SFP
Protocolo de direccionamiento: OSPF, IGRP, RIP, BGP-4, IS-IS, RIP-2, EIGRP
Protocolo de interconexión de datos: Ethernet, Fast Ethernet, Gigabit Ethernet
Red / Protocolo de transporte: L2TP, IPSec

Protocolo de gestión remota: SNMP, Telnet
Alimentación: CA 120/230 V (50/60 Hz)

Características Técnicas:

- Las interfaces de red residen en adaptadores de puertos que proporcionan la conectividad entre los tres buses PCI del ruteador y las redes externas.

- Posee seis ranuras (numeradas del 1 al 6) para los adaptadores de puerto, una ranura para un controlador de entrada/salida y una ranura para el motor de procesamiento de red. Los adaptadores de puerto se pueden ubicar en cualquiera de las seis ranuras disponibles.

- Tiene doble fuente de AC a 120V.

Cabe mencionar que en el NAP.EC aparte de contar con estos equipos, cuenta también con **POLIZAS DE MANTENIMIENTO CISCO SMARTnet** el cual es un servicio de soporte técnico y cambio de partes defectuosas en sitio. También esta póliza es una especie de seguro de protección de sus sofisticados equipos Cisco, ya que si se llegaran a dañar, su inversión está segura, al tener la tranquilidad de que se le sustituirá por otro similar en tan solo unas horas después de notificar al Centro de Atención Técnica (TAC) de la falla.

7.1.2 REQUERIMIENTOS DE SOFTWARE

Cisco IOS se basa fundamentalmente en un modelo de herencia. Cada nuevo paquete hereda todas las características de Cisco IOS Software y servicios disponibles en los paquetes debajo de él, ofreciendo a los clientes una migración clara y ruta de actualización. Como muestra en la Figura 7.1 (Plataforma del IOS de Cisco), se ve claramente que el IOS apto para IPv6 es el Advenced IP Services.

7.1.2.1 ADVANCED IP SERVICES

Combina soporte para datos y voz con capacidades de seguridad y VPN. Es compatible con todas las características y el hardware soportado en el Servicios de SP conjunto de características, y añade soporte para las VPN, IDS, IPv6, y servicios de Cisco IOS Firewall en el conjunto de características de seguridad avanzada

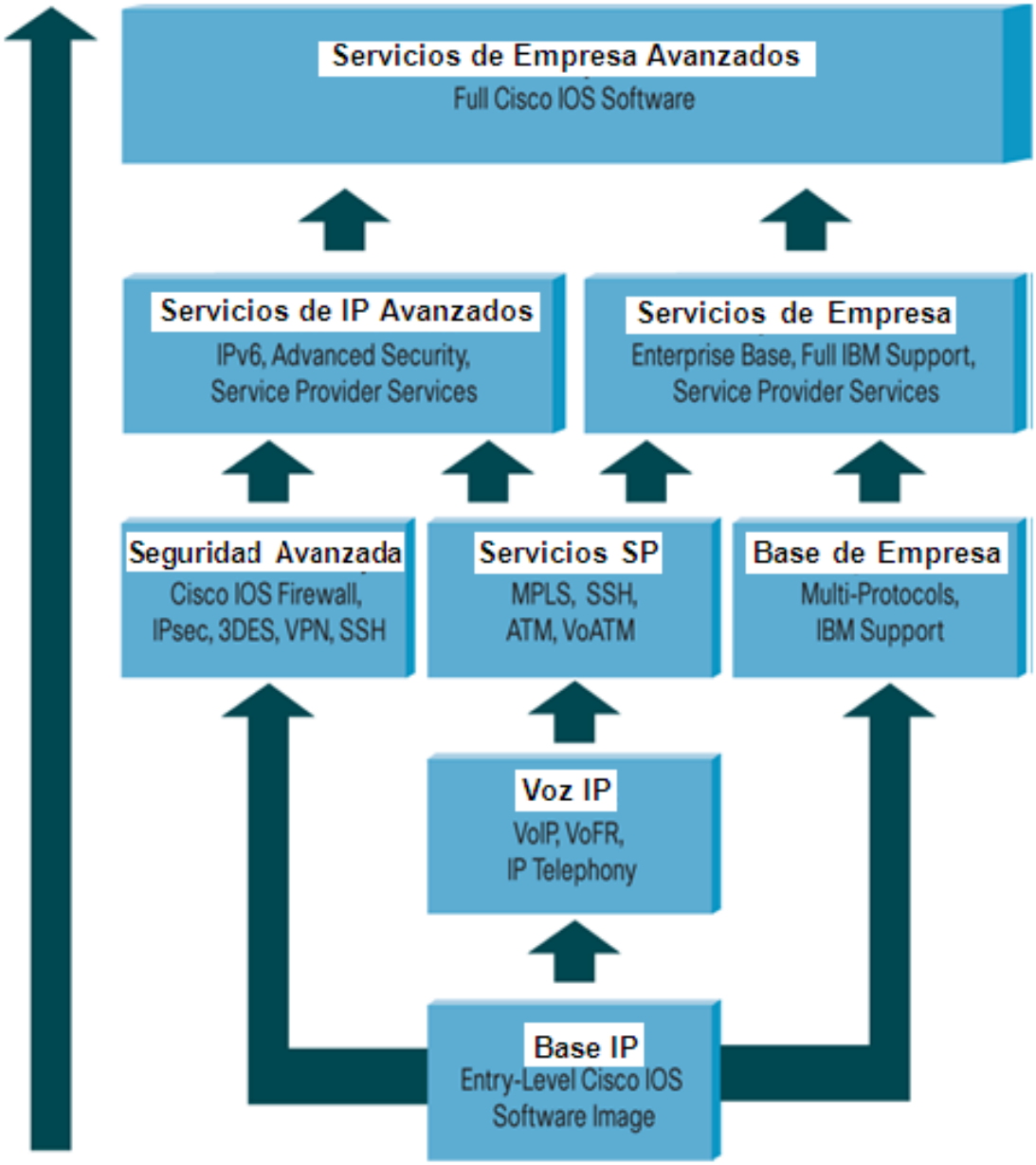


FIGURA 7.46 Plataforma del IOS de Cisco

FUENTE: http. Cisco.com

7.1.2.2 MRTG (MULTI ROUTER TRAFFIC GRAPHER)

En el caso del NAP.EC el software que utiliza para el monitoreo del tráfico es un programa libre (véase detalladamente en el capítulo 5).

7.2 COSTOS NUEVOS REQUERIMIENTOS DE HARDWARE

Se hace innecesaria la adquisición de nuevos equipos, los ya existentes tienen la capacidad de soporte que se necesita para realizar la transición de IPv4 a IPv6.

7.3 COSTOS DE SOFTWARE Y DIRECCIONES IPv6

7.3.1 COSTO DE SOFTWARE

Al igual que el hardware, el software a utilizarse será el mismo, por lo tanto no se va adquirir un nuevo software, el ya existente IOS de Cisco proporciona el rendimiento, la escalabilidad y la seguridad para los productos de Cisco y permite una instalación de redes integrada, centralizada y automatizada. Además, este software ofrece una gestión de redes fácil y sin problemas y proporciona el soporte para una amplia variedad de protocolos, medios de comunicación, servicios y plataformas.

7.3.2 COSTO DE DIRECCIONES IPv6

En la actualidad y hasta nueva resolución del Directorio de LACNIC, las organizaciones que califiquen para recibir bloques de direcciones IPv6 están exoneradas de pago. Esta medida se toma como una forma de promoción de la adopción del IPv6 en la región de cobertura de LACNIC y ante la solicitud de varias organizaciones que hicieron este planteo.

Con esta medida, el directorio de LACNIC intenta dar respuesta a las necesidades de la comunidad de Internet de la región.

7.4 ANÁLISIS COSTO – BENEFICIO

Para estimar el costo, se ha tomado en cuenta básicamente los siguientes parámetros:

- Costo del equipo.
- Costo de la capacitación
- Costo de la implementación

7.4.1 ANÁLISIS DE COSTOS

7.4.1.1 COSTO DEL EQUIPO

Los equipos que actualmente posee el NAP.EC fueron adquiridos hace un año, son de marca Cisco y cumplen con las especificaciones técnicas requeridas para el diseño de la red propuesta. (Ver tabla 7.1)

EQUIPO	CANTIDAD	VALOR TOTAL
Enrutador Cisco 7206VXR	1	$ 22.400,00
Switch Cisco Catalyst 3560G-24TS	1	$ 3.895,00
TOTAL		**$ 26.295,00**

Tabla 7.1 Equipos de NAP.EC

En la tabla 7.2 se presenta el costo del software SERVICIOS IP AVANZADOS (ADVANCED IP SERVICES) para la administración y el software MRTG para el monitoreo de tráfico del NAP.EC.

SOFTWARE	CANTIDAD	VALOR TOTAL
Software Cisco IOS ADVANCED IP SERVICES	1	$ 3.203,20
Software MRTG monitoreo tráfico	1	$ 0
TOTAL		**$ 3.203,20**

Tabla 7.2 Costo de Software

7.4.1.2 COSTO DE LA CAPACITACIÓN

La persona encargada de la Administración del NAP.EC debe recibir una capacitación de dos horas diarias por el lapso de dos meses teniendo un costo de $500 el curso.

Como se observa en la Figura 7.3 muestra el costo de la capacitación y las horas que la persona invierte en asistir al curso.

DETALLE	TIEMPO	VALOR TOTAL
Capacitación	80 Horas	$ 500,00
Horas hombre	80 Horas	$ 240,00
TOTAL		**$ 740,00**

Tabla 7.3 Costos de Capacitación

7.4.1.3 COSTOS OPERATIVOS

De acuerdo a datos proporcionados por el Administrador, los costos operativos del NAP.EC es de aproximadamente $10.000 mensuales.

Existen otros gastos como son los servicios básicos y el arriendo de la oficina. En la tabla 7.4 se presentan dichos gastos.

DETALLE	VALOR MENSUAL (USD)	TOTAL ANUAL (USD)
Arriendo de oficina	$ 1.000,00	$ 1.2000,00
Servicios Básicos	$ 1.300,00	$ 1.5600,00
Suministros de oficina	$ 200,00	$ 2400,00
Servicio de SMARnet	$ 432,58	$ 5.191,00
Gastos varios	$ 600,00	$ 7200,00
TOTAL	**$ 3.532,58**	**$ 4.2391**

Tabla 7.4 Gastos Administrativos

7.4.1.4 COSTO DE IMPLEMENTACIÓN

Para el análisis del costo de la implementación se tomará como parámetro principal el tiempo que lleva la tarea de instalación y configuración.

(Horas hombre - 2 meses / medio tiempo de 1 ingeniero, incluye tiempo de monitoreo posterior, incluye documentación).

También como punto importante NAP.EC tiene el hardware listo para la instalación del sistema operativo, además cuenta con que el implementador (administrador) posee la suficiente experiencia para modificar los archivos de configuración.

DETALLE	TIEMPO IMPLEMENTACIÓN	SUELDO MENSUAL	TOTAL
Administrador	2 meses/medio tiempo	$ 1.000,00	$ 2.000,00
Documentación	2 meses/medio tiempo	$ 200,00	$ 400,00
TOTAL IMPLEMENTACIÓN			**$ 2.400,00**

Tabla 7.5 Costos de Implementación

En la siguiente tabla se presenta el flujo de caja neto del proyecto; donde se considera un período de 3 años, desde el año 2.010 hasta el 2.013.

	INICIO	AÑO 2010	AÑO 2011	AÑO 2012
INGRESOS (USD)				
Servicios	-	$ 2.330,00	$ 2.457,00	$ 2.636,05
TOTAL INGRESOS		$ **2.330,00**	$ **2.457,00**	$ **2.636,05**
EGRESOS (USD)				
Equipos	$ 0			
Software	$ 0			
Capacitación	$ 740,00			
Implementación	$ 2.400,00			
Total Implementación		$ 1.046,67	$ 1.151,34	$ 1.266,47
TOTAL EGRESOS	$ **3.140,00**	$ **1.046,67**	$ **1.151,34**	$ **1.266,47**
FLUJO NETO (USD)	**-** $ **3.140,00**	$ **1.283,33**	$ **1.305,66**	$ **1.369,58**

Tabla 7.6 Flujo Neto del Proyecto

7.4.2 INDICADORES DE RENTABILIDAD

Para obtener una evaluación de la rentabilidad esperada del proyecto se analizan los siguientes indicadores. Estos indicadores son:

Valor Actual Neto (VAN)
Tasa Interna de Retorno (TIR)

7.4.2.1 VALOR ACTUAL NETO (VAN)

Es un procedimiento que permite calcular el valor presente de un determinado número de flujos de caja futuros, originados por una inversión. La metodología consiste en descontar al momento actual (es decir, actualizar mediante una tasa) todos los flujos de caja futuros del proyecto. A este valor se le resta la inversión inicial, de tal modo que el valor obtenido es el valor actual neto del proyecto.

Representa un equivalente de los ingresos netos futuros y presentes del proyecto para realizar el análisis del resultado existen tres alternativas:

- Si el VAN > 0 el proyecto debe ser aceptado
- Si el VAN = 0 para la empresa es igual si se realiza o no el proyecto
- Si el VAN < 0 el proyecto no vale la pena debe ser rechazado.

Para realizar el cálculo se utiliza la siguiente fórmula:

$$\mathbf{VAN} = -\mathbf{I}_0 + \sum_{n=1}^{m} \frac{\mathbf{F}_n}{(1+\mathbf{i})^n}$$

Donde:

I_0 = Inversión Inicial
F_n = Flujos netos.
M = Número de períodos considerados
i = Tasa de interés

La tasa de interés[26] a utilizarse es la vigente en el mercado *i*= 11,82% anual, se considera que no varía esta tasa en los próximos 5 años, tiempo de estudio del proyecto. En la tabla 7.7 se muestran los valores para calcular el VAN.

	INICIO	AÑO 2010	AÑO 2011	AÑO 2012
F_n (USD)	$ 3.140,00	$ 1.283,33	1.305,66	1.369,58
I_0 (USD)	$ 3.140,00			
i (%)	**11,82**			

Tabla 7.7 **Valores para calcular el VAN**

$$VAN = 3.140,00 + 1.283,\frac{33}{(1+0,1182)^1} + 1.305,\frac{66}{(1+0,1182)^2} + 1.369,\frac{58}{(1+0,1182)^3}$$

$$VAN = \$\,31,39$$

Como el VAN= 31,39 USD es mayor que cero, se concluye que el proyecto si es rentable.

7.4.2.2 TASA INTERNA DE RETORNO (TIR)

La Tasa Interna de Retorno es la tasa de interés que iguala en el tiempo los ingresos y egresos de un flujo de caja; es decir, la TIR es el tipo de interés que anula el VAN de una inversión (VAN=0). En términos generales un proyecto es rentable cuando la TIR es mayor que la tasa de interés mínima vigente en el mercado.

La fórmula que permite calcular la TIR es:

$$TIR = -I_0 + \sum_{n=1}^{m} \frac{F_n}{(1+r)^n} = 0$$

Donde:

I_0 = Inversión inicial

F_n = Flujos netos para el periodo n

26. Fuente: http://www.bce.fin.ec/ (Banco Central del Ecuador).

m = Número de períodos totales

r = Tasa interna de retorno

$$TIR = -3.140,00 + 1.283,\frac{33}{(1+r)^1} + 1.305,\frac{66}{(1+r)^2} + 1.369,\frac{58}{(1+r)^3}$$

$$TIR = r = 0.53\% = 53\%$$

Como el TIR = 53% es mayor que la taza de interés mínima utilizada en el proyecto de i(%)=11,82% entonces el proyecto es viable.

7.4.3 RELACIÓN BENEFICIO COSTO (B/C)

La relación de beneficio costo determina la rentabilidad del proyecto, el resultado de esta relación expresa el dinero ganado en cada dólar que se invierte en el proyecto.

Esta relación de calcula de la siguiente manera:

$$\frac{B}{C} = \frac{\sum_1^n VAN_n}{I_0}$$

Donde:

VAN = Valor actual neto VAN = 31,39 USD

$$\frac{B}{C} = 31,\frac{39}{3}.140,00$$

n = Duración en años del proyecto

I_0 = Inversión inicial

B/C = $ 0,009367

Para el sistema analizado se tiene una relación Costo - Beneficio: por cada dólar invertido en el proyecto se gana **$0,009367.**

7.5 RECUPERACIÓN DE LA INVERSIÓN

7.5.1 PERIODO DE RECUPERACIÓN DE LA INVERSIÓN (PRI)

El período de recuperación de la inversión es el tiempo necesario para que el proyecto recupere el capital invertido; es decir, entre más corto sea el periodo para la recuperación de lo invertido más viable es el proyecto.

Una forma de calcular el PRI[27] es ir acumulando los flujos netos hasta llegar a cubrir la inversión. Para el proyecto en estudio la inversión es de 32.638,20 USD. En la tabla 7.8, se muestra el flujo neto para cada año, así como los flujos netos acumulados.

En la tabla 7.8, se observa que el flujo neto acumulado en el año 2.012 es mayor que la inversión, por lo tanto el período de recuperación de la inversión se encuentra entre el año 2.011 y el año 2.012.

Para determinar el PRI con mayor exactitud se escoge el flujo neto del año 2.011 donde aún no se cubre la inversión y se lo resta de la inversión.

AÑO	FLUJO NETO (USD)	FLUJO NETO ACUMULADO (USD)
2010	$ 1.283,33	$ 1.283,33
2011	$ 1.305,66	$ 2.588,99
2012	$ 1.369,58	$ 3.958,57

Tabla 7.8 Datos para calcular el PRI

En la tabla anterior, se observa que en el año 2012 el flujo neto acumulado es mayor que la inversión, por lo tanto el periodo de recuperación de la inversión se encuentra en el año 2012.

27. Período de recuperación de la inversión.- es el tiempo necesario para que el proyecto recupere el capital invertido

CONCLUSIONES Y RECOMENDACIONES.

- El grupo Internet Research Task Force (IRTF) está buscando una nueva arquitectura de routing que haga posible escalar la capacidad de Internet para soportar los potenciales miles de millones de nuevos usuarios en países en desarrollo. Uno de los temas a debate en IRTF –organización hermana de Internet Engineering Task Force (IETF)– es el modo en que operan los routers centrales (backbone) de la Red, que –propiedad de los operadores, grandes empresas y agencias gubernamentales– ejecutan Border Gateway Protocol (BGP) para intercambiar información de routing entre las muchas redes interconectadas que forman Internet.

- Al hablar de IPv6, se encuentran involucrados aspectos importantes inherentes a este concepto, siendo uno de los más importantes el enrutamiento a través de los protocolos tanto internos como externos.

- La mayoría de los protocolos de enrutamiento para IPv6 se construyen en base a sus pares de IPv4, es así que el mecanismo fundamental de OSPF para IPv4 permanece sin cambios profundos en IPv6 y que el soporte BGP para IPv6 deriva de la capacidad de BGP-4 para intercambiar información entre los protocolos de la capa de red.

- Además de solventar la escasez de direcciones IP, el protocolo IPv6 ha sido creado, desde un inicio, con la seguridad y eficiencia como objetivos, medidas como la implantación de IPsec, el nuevo diseño del paquete o la manera de asignar las direcciones IP son la prueba de ello.

- El EGP para IPv6 es BGP-4, ya que permite superar algunos problemas tal como el de los bucles que pueden aparecer con EGP.

- Al encontrarse ante una situación de utilizar un enrutador y no se cuenta con el dinero suficiente como para poder adquirir un equipo sofisticado (CISCO), y si los requerimientos no son muy exigentes, se puede solventar el problema utilizando un software de simulación, como lo es GNS3.

- El BGP o Border Gateway Protocol es un protocolo mediante el cual se intercambian prefijos los ISP registrados en Internet. Este protocolo requiere un router que tenga configurado cada uno de los vecinos que intercambiarán información de las rutas que cada uno conozca.

RECOMENDACIONES

- Direccionamiento IPv4 e IPv6: se debe utilizar un solo bloque de direcciones IPv4 e IPv6 en Doble Pila (DUALSTACK), cada Red Regional deberá definir qué direcciones con las que cuenta utilizará para la conexión.

- Protocolo de enrutamiento; el proveedor de cada red regional debe estar en la capacidad de gestionar el enrutamiento de la información generada por cada proveedor hacia la Red utilizando el protocolo de enrutamieto BGP.

- Una precaución que hay que tomar al utilizar BGP es el control de los AS (Sistemas Autónomos) que no son más que sistemas o redes independientes que se desean comunicar.

- Obtener conocimiento de la administración de sistemas IPv6, ya que, aunque en la actualidad se pueda bloquear todo el tráfico IPv6 o se disponga de direcciones IPv4, en el futuro será cada vez más necesario porque los proveedores integrarán sus servicios con IPv6.

- Disponer de dispositivos de seguridad, es recomendable, definir un subconjunto de reglas y políticas de seguridad diferenciadas para el tráfico IPv6, y herramientas de gestión de red que sean capaces de analizar y, en caso de que sea necesario, bloquear el flujo de datos IPv6 y los túneles o mecanismos de transición IPv6.

BIBLIOGRAFÍA

LIBROS:

- Arquitecturas de enrutamiento en Internet, 2da Edición
  Sam Halabi – Danny McPherson

- Internetworking with TCP/IP, Volúmen 1
  Douglas E. Comer

- BGP4: Inter-Domain Routing in the Internet
  J.Stewart

- Enrutamiento TCP/IP, Volúmen 1
  Jeff Doyle

- Redes de Computadoras, 4ta Edición
  Tanenbaum Andrew

- Fundamentos de Ingeniería económica, 4ta Edición
  Baca Urbina Gabriel

ORGANIZACIONES INTERESANTES:

- Asociación de empresas proveedoras de servicios de Internet, valor agregado, portadores y tecnologías de la información (AEPROVI): www.aeprovi.org.ec

- Registros de Direcciones de Internet para Latinoamérica y el Caribe (LACNIC): www.lacnic.net

- Internet Engineering Task Force (IETF): www.ietf.org

- Internet Assigned Numbers Authority (IANA): www.iana.org
- Internet2: www.internet2.edu
- Cisco Connection Online (CCO): www.cisco.com

PÁGINAS WEB:

- http://www.cu.ipv6tf.org/pdf/Tutorial%20de%20IPV6.pdf
- http://www.freebsd.org/doc/es/books/handbook/network-ipv6.html
- http://lacnic.net/documentos/ipv6tour2009/dominicana/ipv6tour-do-rp.pdf
- http://technet.microsoft.com/es-es/library/cc736336(WS.10).aspx
- http://www.itu.int/ITU-D/finance/work-cost-tariffs/events/tariff-seminars/SantoDomingo-10/pdf/Session13_OMesano_IPv6Transition.pdf
- http://www.elmundo.es/imasd/ipv6/queesipv6.html
- http://es.wikipedia.org/wiki/Border_Gateway_Protocol
- http://ws.edu.isoc.org/workshops/2004/CEDIA2/material/bgp.pdf
- http://www.bgp4.as/
- http://www.elpais.com/articulo/internet/protocolo/BGP/elpeputec/20080827elpepunet_9/Tes

GLOSARIO DE TÉRMINOS

A

AFRINIC *(American Regional Internet Registry - Registro Regional de recursos numéricos de Internet para Africa)*
Es una organización no gubernamental, sin fines de lucro que se encarga de la asignación de recursos de Internet para el África.

APNIC *(Asia Pacific Network Information Centre - Centro de Información de Redes Asiáticas y del Pacífico)*
Es una organización sin fines de lucro, basada en membresía, cuyos miembros incluyen a proveedores de servicios Internet, los Registros Nacionales de Internet, y otras organizaciones similares.

ARIN *(American Registry for Internet Numbers - Registro Americano de Números para Internet)*
Administra la distribución de recursos numéricos de Internet, incluyendo IPv4 y IPv6 espacio de direcciones y números de AS .

ASN *(Autonomous System Number - Sistema de Número Autónomo)*
Es un conjunto de redes y dispositivos que se encuentran administrados por una sola entidad (o en algunas ocasiones varias) bajo una política en común.

ATM *(Modo de Transferencia Asincrónica)*
Es una tecnología de conmutación de red que utiliza celdas de 53 bytes, utilizada tanto para LAN como para WAN, soporta voz, vídeo y datos en tiempo real y obre la misma infraestructura.

B

BGP (*Border Gateway Protocol - Protocolo de Gateway Fronterizo)*
Es un protocolo mediante el cual se intercambia información de encaminamiento

entre sistemas autónomos.

C

CIDR *(Classless InterDomain Routing - Encaminamiento InterDominios sin Clases)*
Es la simplificación de varias direcciones de redes o subredes en una sola dirección IP Patrón que cubra todo ese esquema de direccionamiento IP.

CPU *(Central Processing Unit - Unidad Central de Proceso)*
La CPU es el cerebro del ordenador. A veces es referido como el procesador central, en donde se producen la mayoría de los cálculos.

D

DNS *(Domain Name System - Sistema de Nombre de Dominio)*
Es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet.

DHCPv6 *(Dynamic Host Configuration Protocol for IPv6 - Protocolo de Configuración Dinámica de Hosts para IPv6)*
Es una extensión de BOOTP que define un protocolo para que transmita la información sobre la configuración a los sistemas host de una red.

E

EGP *(Exterior Gateway Protocol – Protocolo de Pasarela Exterior)*
Es el protocolo utilizado para el intercambio de información de encaminamiento entre pasarelas exteriores (que no pertenezcan al mismo Sistema Autónomo AS).

EIGRP *(Extended Internal Gateway Routing Protocol – Protocolo de Enrutamiento de Gateway Interior Mejorado)*
Es un protocolo de enrutamiento por vector-distancia avanzado, pero también actúa como protocolo del estado de enlace en la manera en que actualiza a los vecinos y

mantiene la información de enrutamiento.

Ⓖ

GUI *(Graphical User Interface - Interfaz Gráfica de Usuario)*

Conjunto de formas y métodos que posibilitan la interacción de un sistema con los usuarios utilizando formas gráficas e imágenes. Con formas gráficas se refiere a botones, íconos, ventanas, fuentes, etc. los cuales representan funciones, acciones e información.

IANA *(Internet Assigned Number Authority - Autoridad de Asignación de Números en Internet)*

Es responsable de la coordinación mundial de la raíz de DNS, las direcciones IP, y otros recursos de protocolo de Internet.

ICANN *(*Internet Corporation for Assigned Names and Numbers - *Corporación de Internet para la Asignación de Nombres y Números)*

Es una organización que opera a nivel internacional, siendo el responsable de asignar las direcciones del protocolo IP, de los identificadores de protocolo, de las funciones de gestión del sistema de dominio y de la administración del sistema de servidores raíz.

ICMP *(Internet Control Message Protocol - Protocolo de Mensajes de Control de Internet)*

Es un protocolo que permite administrar información relacionada con errores de los equipos en red. Si se tienen en cuenta los escasos controles que lleva a cabo el protocolo IP, ICMP no permite corregir los errores sino que los notifica a los protocolos de capas cercanas.

IETF *(Internet Engineering Task Force - Grupo de Tareas de Ingeniería de Internet)*

Organización de técnicos que administran tareas de ingeniería de

telecomunicaciones, principalmente de Internet.

IOS *(Internetwork Operating System - Sistema Operativo de Interconexión de Redes)*

Sistema operativo creado por Cisco Systems para programar y mantener equipos de interconexión de redes informáticas como switches (conmutadores) y routers.

IP *(Internet Protocol - Protocolo de Internet)*

Es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red.

IPsec *(Internet Protocol Security - Seguridad del Protocolo de Internet*

Es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos.)

IPv4 *(Internet Protocol v4 - Protocolo de Internet versión 4)*

Versión 4 del protocolo IP (Internet Protocol). Es el estándar actual de Internet para identificar dispositivos conectados a esta red. Utiliza direcciones IP de 32 bits, lo cual limita la cantidad de direcciones a 4.294.967.296 (2 elevado a 32).

IPv6 *(Internet Protocol v6 - Protocolo de Internet versión 6)*

Es una nueva versión de IP, diseñada para reemplazar a la versión 4 (IPv4) actualmente en uso dominante.

IPX *(Internet Packet Exchange - Intercambio de Paquetes interred).*

Protocolo para el intercambio de paquetes entre aplicaciones dentro de una red Netware. Actualmente este protocolo esta en desuso y sólo se utiliza para juegos en red antiguos.

ISP *(Internet Service Provider - Proveedor de Servicios de Internet)*

Es una empresa que brinda conexión a Internet a sus clientes. Un ISP conecta a sus usuarios a Internet a través de diferentes tecnologías como DSL, Cable módem, GSM, Dial-up, Wifi, entre otros.

IS-IS *(Intermediate System to Intermediate System - Sistema intermedio al sistema intermedio)*
Es un protocolo usado por los dispositivos de la red para determinar la mejor manera de remitir datagramas o los paquetes con a red paquete-basada, un proceso llamado encaminamiento.

K

KDE *(K Desktop Environment - Entorno de Escritorio K)*

Es un proyecto de software libre para la creación de un entorno de escritorio e infraestructura de desarrollo para diversos sistemas operativos como GNU/Linux, Mac OS X, Windows, etc.

L

LACNIC *(Latin American and Caribbean Internet Address Registry - Registro Latino-Americano y Caribeño de Direcciones de Internet)*
Administran las Direcciones IP versión 4 y versión 6, Números de Sistemas Autónomos, DNS Reverso, y otros recursos de red para la región.

LAN *(Local Área Network - Red de Área Local)*
Es un sistema de comunicación entre computadoras que permite compartir información, con la característica de que la distancia entre las computadoras debe ser pequeña.

M

MAC *(Media Access Control - Control de Acceso al Medio)*
Es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una ethernet de red. Se conoce también como la dirección física en cuanto identificar dispositivos de red.

MTU *(Maximum Transmission Unit o Unidad Máxima de Transferencia)*
Es un parámetro que indica el tamaño máximo que debe tener un datagrama para que sea transmitido por una interfaz IP sin que necesite ser fragmentado en unidades más pequeñas. El MTU debe ser superior al datagrama más grande que deseemos transmitir para que no sea fragmentado.

N

NAP *(Network Access Point - Punto de Acceso a la Red)*
Es un lugar físico donde varios ISPs se conectan, para poder enrutar e intercambiar información entre ellos mismos u otros terceros, dependiendo de los tipos de acuerdos, sean estos económicos u asociativos, que se hayan establecido entre sus miembros.

NAT *(*Network Address Translation - *Traducción de Dirección de Red)*
Es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles.

NIR *(Registro de Internet Nacional)*
Distribuye, principalmente, los recursos de Internet a sus miembros o constituyentes, los cuales generalmente son LIRs.

NVRAM *(Non-volatile random access memory - Memoria de acceso aleatorio no volátil)*
Es un tipo de memoria de acceso aleatorio que, como su nombre indica, no pierde la información almacenada al cortar la alimentación eléctrica.

O

OSI *(Open Systems Interconnection - Interconexión de Sistemas Abiertos)*
Es un lineamiento funcional para tareas de comunicaciones y, por consiguiente, no especifica un estándar de comunicación para dichas tareas.

OSPF *(Open Shortest Path First - Primero la Ruta Libre más Corta)*
Propone el uso de rutas más cortas y accesibles mediante la construcción de un mapa de la red mediante bases de datos con información sobre sistemas locales y vecinos.

Q

Qemu
Es un emulador de procesadores basado en la traducción dinámica de binarios (conversión del código binario de la arquitectura fuente en código entendible por la arquitectura huésped). QUEMU también tiene capacidades de virtualización dentro de un sistema operativo, ya sea Linux, Windows, etc.

R

RAM *(Random Access Memory - Memoria de Acceso Aleatorio)*
Es donde el computador guarda los datos que está utilizando en el momento presente. El almacenamiento es considerado temporal por que los datos y programas permanecen en ella mientras que la computadora este encendida o no sea reiniciada.

RIP *(Routing Information Protocol - Protocolo de encaminamiento de información)*
Es un protocolo de vector-distancia que utiliza el número de saltos como métrica. RIP es ampliamente utilizado para el encaminamiento del tráfico en la Internet mundial.

RIPE NCC *(Réseaux IP Europeer Network Coordination - Centro de Coordinación de redes IP europeas)*
Proporciona soporte técnico y administrativo a Redes IP Europeas, Oriente Medio y partes de Asia Central.

RIR *(Regional Internet Registry - Registro de Internet Regional)*
Es una organización que supervisa la asignación y registro de numeración de Internet dentro de una región particular del mundo.

ROM *(Read Only Memory - Memoria de Solo Lectura)*
Es un medio de almacenamiento utilizado en los ordenadores y otros dispositivos electrónicos. Los datos almacenados en la ROM no se pueden modificar al menos no de manera rápida o fácil, y es poco probable que requiera actualizaciones frecuentes.

RTP *(Real time Transport Protocol - Protocolo de Transporte de Tiempo real)*
Es un protocolo de nivel de sesión utilizado para la transmisión de información en tiempo real, como por ejemplo audio y vídeo en una video-conferencia.

RTCP *(Real Time Control Protocol - Protocolo de Control en Tiempo Real)*
Es un protocolo de comunicación que proporciona información de control que está asociado con un flujo de datos para una aplicación multimedia (flujo RTP).

S

SPF *(Shortest path first - Primero la ruta más corta)*
Algoritmo de enrutamiento que realiza iteraciones sobre la longitud de la ruta para determinar el spaning tree (árbol de extensión) de ruta más corta. Comúnmente utilizado en los algoritmos de enrutamiento de estado de enlace. A veces denominado algoritmo de Dijkstra.

T

TCP/IP *(Transmission Control Protocol / Internet Protocol - Protocolo de control de transmisión / Protocolo de Internet)*
Se le llama TCP/IP, a la familia de protocolos que nos permite estar conectados a la red Internet.

Este nombre viene dado por los dos protocolos estrella de esta familia:

- El protocolo TCP, funciona en el nivel de transporte del modelo de referencia OSI, proporcionando un transporte fiable de datos.
- El protocolo IP, funciona en el nivel de red del modelo OSI, que nos permite encaminar nuestros datos hacia otras maquinas.

U

UDP (*User Datagram Protocol - Protocolo de datagrama de usuario)*
Es un protocolo no orientado a conexión de la capa de transporte del modelo TCP/IP. Este protocolo es muy simple ya que no proporciona detección de errores (no es un protocolo orientado a conexión).

V

VLSM *(Variable Length Subnet Mask - Máscara de Subred de Tamaño Variable)*
Es una técnica que permite dividir subredes en redes más pequeñas pero la regla que hay que tener en consideración siempre es que se utilice VLSM es que solamente se puede aplicar esta técnica a las direcciones de redes/subredes que no están siendo utilizadas por ningún host.

W

WAN (*Wide Área Network - Red de Área Amplia)*
Es una red de comunicaciones utilizada para conectar ordenadores y otros dispositivos a gran escala. Las conexiones pueden ser privadas o públicas.

WCCP *(Web Cache Control Protocol)*
Propietario de Cisco, redirige tráfico Web desde un router al motor de caché de Cisco.

X

xDSL *(Digital Subscriber Line - Línea del Suscriptor Digital)*

Es el término genérico que se aplica a los protocolos ADSL, HDSL, SDSL, IDSL y VDSL

ANEXOS

.
Por último, se presentan los anexos que dan soporte al proyecto de titulación.

ANEXO 1:

Muestra los comandos básicos para configurar un router.

ANEXO 2:

Comandos de configuración de BGP.

ANEXO 3:

Comandos de configuración de IPv6.

ANEXO 1

1.5 COMANDOS BÁSICOS PARA CONFIGURAR UN ROUTER.

CAMBIO ENTRE MODOS

```
router>
router> enable (pasa al Modo Exec Privilegiado)
router#
router# disable (regresar al Modo Usuario)

router> enable (pasa al Modo Exec Privilegiado)
router#
router# exit (vuelve a al Modo Exec Usuario)

router> enable
router#
router# config terminal (pasa al Modo Configuración Global)
router(config)#
router(config)# exit ó CTRL+z (vuelve al Modo Privilegiado)
router#
```

- **Cambiar el nombre al router**

```
router> enable
router# configure terminal
router(config)# hostname [routerA]
routerA(config)# Ctrl + z
routerA
```

- **Configurar contraseñas “enable password”**

```
routerA> enable
routerA# configure terminal
routerA(config)# enable password [password]
routerA(config)# Ctrl +z
routerA
```

- **Configurar contraseñas “enable secret”**

```
routerA> enable
routerA# configure terminal
routerA(config)# enable secret [password]
routerA(config)# Ctrl + z
routerA
```

- **Configurar terminal (vty)**

```
routerA> enable
routerA# config terminal
routerA(config)# line vty 0 4
routerA(config-line)# login (habilita la contraseña)
routerA(config-line)# password [password]
routerA(config-line)# exit
routerA(config)#
```

- **Configurar Consola**

```
routerA> enable
routerA# config terminal
routerA(config)# line console 0
routerA(config-line)# login (habilita la contraseña)
routerA(config-line)# password [password]
routerA(config-line)# exit
routerA(config)#
```

- **Configurar auxiliar**

```
routerA> enable
routerA# config terminal
routerA(config)# line auxiliar 0
routerA(config-line)# login (habilita la contraseña)
routerA(config-line)# password [password]
routerA(config-line)# exit
routerA(config)#
```

- **Configuración de mensaje del día**

```
routerA> enable
routerA# config terminal
routerA(config)# banner login#
Enter TEXT message. End with the carácter ´#´
Mensaje#
routerA(config-line)# Ctrl + z
routerA(config)#
```

- **Configurar interfaces ethernet o fast ethernet**

```
routerA> enable
routerA# config terminal
```

```
routerA(config)# interface fastethernet 0/0
routerA(config-if)# ip address 192.168.0.1 255.255.255.0
routerA(config-if)# no shutdown (levanta la interfaz)
routerA(config-if)# description lan (asigna un nombre a la
interfaz)
routerA(config-if)# exit
routerA(config)#
```

- **Configurar interfaces serial como DTE**

```
routerA> enable
routerA# config terminal
routerA(config)# interface serial 0/0
routerA(config-if)# ip address 10.0.0.1 255.0.0.0
routerA(config-if)# no shutdown (levanta la interfaz)
routerA(config-if)# description red (asigna un nombre)
routerA(config-if)# exit
routerA(config)#
```

- **Configurar interfaces serial como DCE**

```
routerB> enable
routerB# config terminal
routerB(config)# interface serial 0/1
routerB(config-if)# ip address 10.0.0.2 255.0.0.0
routerB(config-if)# clock rate 56000 (configura la
sincronización entre los enlaces)
routerB(config-if)# no shutdown (levanta la interfaz)
routerB(config-if)# description red (asigna un nombre)
routerB(config-if)# exit
routerB(config)#
```

- **Configuración del protocolo**

```
routerB> enable
routerB# config terminal
routerB(config)# router rip
routerB(config-if)# Ctrl+z
routerB#
```

- **Configuración de rutas estáticas**

```
routerB> enable
routerB# config terminal
routerB(config)# ip router ip_[red_origen] [máscara_destino]
[ip_interface_destino]
```

```
routerB(config-if)# Ctrl+z
routerB#
```

- **Configuración de redes directamente conectadas**

```
routerB> enable
routerB# config terminal
routerB(config)# router [protocolo]
routerB(config-if)# network [dirección]
routerB# Ctrl+z
routerB#
```

- **Comandos de la secuencia de arranque**

```
routerB> enable
routerB# config terminal
routerB(config)# boot system rom
routerB(config)# Ctrl+z
routerB#
```

- **Guardar la configuracion activa del router**

```
RouterB# copy running-config startup-config
```

- **Copia de seguridad sin solicitud de confirmación**

```
RouterB# write
```

- **Reiniciando al router**

```
Router# reload
```

COMANDOS DE INFORMACIÓN

- **routerB# show running-config**

Muestra el archivo de configuración actual del router.

- **routerB# show version**

Permite mostrar información sobre la configuración de hardware del sistema y sobre el ios.

- **routerB# show processes**

Muestra los procesos activos

- **routerB# show protocols**

Muestra los protocolos configurados de la capa 3 del modelo OSI

- **routerB# show memory**

Muestra las estadísticas de memoria del router

- **RouterB# show interface**

Mostrar información y estadísticas sobre una interfaz

- **RouterB# show ip route**

Mostrar la tabla de enrutamiento ip

ANEXO 2

3.9 COMANDOS DE CONFIGURACION DE BGP SOBRE EQUIPAMIENTO MARCA CISCO

auto sumary (bgp).- Este comando de configuración del router para establecer el comportamiento predeterminado del resumen automático de las rutas de subred en las rutas al nivel de red.

Utilice la forma no de este comando si quiere desactivar esta función y enviar información de ruta subprefijada a través de los límites clásicos de la red.

```
Router(config-router)#no auto-summary
```

clear ip bgp.- Utilice este comando EXEC cuando arranque el sistema para reiniciar una conexión BGP usando la reconfiguración del software BGP

```
Router# clear ip bgp 10.0.0.1
```

clear ip bgp dampening.- Utilice este comando EXEC para limpiar la ruta BGP de información relativa al dampening y mostrar las rutas suprimidas.

clear ip bgp flap-statistics.- Se utiliza este comando EXEC para limpiar las estadisticas de fluctuación BGP.

clear ip bgp peer-group.- Utilice este comando EXEC para eliminar a todos los miembros de un grupo de iguales BGP.

clear ip prefix-list.- Utilice este comando de configuración del router para reiniciar la cuenta de saltos de las entradas en la lista de prefijos.

default-information originate (bgp).- Utilice este comando de configuracion del router para permitir la redistribución de red 0.0.0.0 en BGP. Utilice la forma no de este comando si quiere desactivar esta función.

distribute- list in.- Utilice este comando de configuración del router para filtrar las redes recibidas en actualizaciones.

distribute- list out.- Utilice este comando de configuración de un router para suprimir las redes publicadas en las actualizaciones.

ip as-path acces-list.- Utilice este comando de configuración global para definir la lista de acceso relacionada con BGP.

ip bgp-community new-format.- Utilice este comando de configuración global

para visualizar las cominidades BGP en el formato AA:NN (sistema autonomo-numero de comunidad/numero de 2 bytes).

Utilice la forma no de este comando si quiere volver a habilitar el formato de visualización previo para las comunidades BGP (NN:AA).

ip community –list.- Utilice este comando de configuración global para crear una lista de comunidad para BGP y controlar su acceso. Utilice la forma no de este comando para borrar la lista de comunidad.

ip prefix-list.- Utilice este comando de configuración global para crear una entrada en una lista de prefijos. Utilice la forma no de este comando para eliminar dichas descripciones.

ip prefix-list description.- Utilice este comando de configuración global para añadir descripciones de texto a una lista de perfijos. Utilice la forma no de este comando para eliminar dichas descripciones.

ip prefix.list sequense-number.- Utilice este comando de configuración global para habilitar la generación de secuencia de números para las entradas en una lista de prefijos.

match as-path.- Utilice este comando de configuración del mapa de ruta para equiparar una lista de acceso de rutas del sistema autónomo BGP. Utilice la forma no de este comando para borrar una entrada de la lista de entradas.

match community-list.- Utilice este comando de configuración del mapa de ruta para equiparar una comunidad BGP. Utilice la forma no de este comando para borrar una entrada de la lista de comunidad.

neighbor advertisement –interval.- Utilice este comando de configuración del router para establecer el intervalo mínimo entre los envíos de actualizaciones de enrutamientos BGP.

neighbor default-originate.- Utilice este comando de configuración del router para permitir que un portavoz BGP (el router local) envíe la ruta predeterminada 0.0.0.0 a un vecino y que la utilice como ruta predeterminada. Utilice la forma no de este comando para no enviar una ruta como predeterminada.

neighbor description.- Utilice este comando de configuración del router para asociar una descripción con un vecino. Utilice la forma no de este comando para borrar la descripción.

neighbor distribute-list.- Utilice este comando de configuración del router para distribuir información de un vecino BGP como se especifica en una lista de acceso. Utilice la forma no de este comando para borrar una entrada.

neighbor ebgp-multihop.- Utilice este comando de configuración del router para aceptar e intentar conexiones BGP con iguales externos que residan en redes que

no están conectadas directamente. Utilice la forma no de este comando si quiere volver al estado predeterminado.

```
Router(config-router)#
neighbor {ip-address|peer-group-name} ebgp-multihop
```

neighbor filter-list.- Utilice este comando de configuración del router para configurar un filtro BGP. Utilice la forma no de este comando para deshabilitar esta función.

neighbor maximum-prefix.- Utilice este comando de configuración del router para controlar el número de prefijos que puede recibir un vecino. Utilice la forma no de este comando para deshabilitar esta función.

neighbor next-hop-self.- Utilice este comando de configuración del router para desactivar el proceso de próximo salto de las actualizaciones BGP en el *rol/ter.* Utilice su forma no para desactivar esta función.

```
Router(config-router)#
neighbor {ip-address|peer-group-name} next-hop-self
```

neighbor password.- Utilice este comando de configuración del router para permitir autenticación Boletín de mensajes 5 (MDS) en una conexión TCP entre dos iguales BGP. Utilice la forma no de este comando para deshabilitar esta funciÓn.

neighbor peer-group (assigning members).- Utilice este comando de configuración del router para configurar un vecino como miembro de un grupo de iguales. Utilice la forma no de este comando si quiere eliminar a un vecino del grupo de iguales.

neighbor peer-group (creating).- Utilice este comando de configuración del router para crear un grupo de iguales BGP. Utilice la forma no de este comando para eliminar un grupo de iguales *y* todos sus miembros.

```
Router(config-router)#
Neighbour peer-group-name peer-group
```

neighbor prefix-list.- Utilice este comando de configuración del router para distribuir información sobre vecinos BGP como se especifica en una lista de prefijos. Utilice la forma no de este comando para eliminar una entrada.

neighbor remote-as.- Utilice este comando de configuración del router para añadir una entrada a la tabla de vecinos BGP. Utilice la forma no de este comando para eliminar una entrada de esta tabla.

neighbor route-map.- Utilice este comando de configuración del router para aplicar un mapa de la ruta a las rutas entrantes *o* salientes. Utilice la forma de este comando para borrar un mapa de ruta.

neighbor route-reflector-client.- Utilice este comando de configuración del router para configurar el router como un reflector de ruta BGP, *y* además configurar al vecino especificado como su cliente. Utilice la forma no de este comando si quiere indicar que el vecino no es un cliente. Cuando todos los clientes están deshabilitados, el router local no será mayor que un reflector de ruta.
neighbor send-community.- Utilice este comando de configuración del router para especificar que a un vecino BGP se le debería enviar un atributo de "comunidades". Utilice la forma no de este comando para borrar una entrada.

neighbor shutdown.- Utilice este comando de configuración del router para deshabilitar un vecino o un grupo de iguales. Utilice la forma no de este comando para rehabilitar el vecino o el grupo de iguales.

neighbor soft-reconfiguration.- Utilice este comando de configuración del router para configurar el software Cisco IOS para que pueda empezar a almacenar actualizaciones. Utilice la forma no de este comando para no almacenar las actualizaciones recibidas.

neighbor timers.- Utilice este comando de configuración del router para establecer los temporizadores para un igual BGP específico o para un grupo de iguales. Utilice la forma no de este comando para borrar los temporizadores de un igual BGP específico o de un grupo de iguales.

neighbor update-source.- Utilice este comando de configuración del router para que el software Cisco IOS permita que las sesiones BGP internas usen cada interfaz operacional en las conexiones TCP. Utilice la forma no de este comando para restablecer la asignación de la interfaz a la interfaz más próxima, también llamada la mejor dirección local.

neighbor version.- Utilice este comando de configuración del router para configurar el software Cisco lOS para que acepte sólo una versión BGP particular. Utilice la forma no de este comando para usar el nivel de la versión predeterminada de un vecino.

neighbor weight.- Utilice este comando de configuración del router para asignar un ancho a la conexión de un vecino. Utilice la forma no de este comando si quiere eliminar la asignación de un ancho.

network (BGP).- Utilice este comando de configuración del router para especificar la lista de redes en un proceso de enrutamiento BGP. Utilice la forma no de este comando para eliminar una entrada.

network backdoor.- Utilice este comando de configuración del router para especificar una ruta de puerta trasera a un router fronterizo BGP que proporcionará una mejor información sobre la red. Utilice la forma no de este comando para eliminar una dirección de la lista.

network weight.- Utilice este comando de configuración del router para asignar una anchura absoluta a una red SGP. Utilice la forma no de este comando para

eliminar una entrada.

router bgp.- Utilice este comando de configuración global para configurar el proceso de enrutamiento BGP. Utilice la forma no de este comando para eliminar un proceso de enrutamiento.
set as-path.- Utilice este comando de configuración del mapa de ruta para modificar la ruta de un sistema autónomo para rutas BGP. Utilice la forma no de este comando si no quiere modificarla.

set comm-list delete.- Utilice este comando de configuración del router para eliminar comunidades del atributo de comunidad de una actualización entrante o saliente. Utilice la forma no de este comando si quiere negar un comando set comm-list delete anterior.

set community.- Utilice este comando de configuración del mapa de ruta para establecer el atributo BGP COMMUNITIES. Utilice la forma no de este comando para borrar una entrada.

set dampening.- Utilice este comando de configuración del mapa de ruta para establecer los factores de dampening de la ruta BGP. Utilice la forma no de este comando para deshabilitar esta función.

set ip next-hop (BGP).-Utilice este comando de configuración del mapa de ruta para indicar la salida de los paquetes que pasan una clausula de coincidencia de un mapa de ruta en una política de enrutamiento. Utilice la forma no de este comando para borrar una entrada.

set metric-type internal.- Utilice este comando de configuración del mapa de ruta para establecer el valor MED en los prefijos publicados a los vecinos EBGP (Protocolo de gateway fronterizo externo) para coincidir con el métrico IGP (Protocolo de gateway interno) del próximo salto. Utilice la forma no de este comando para volver al estado predeterminado.

set origin (BGP).- Utilice este comando de configuración del mapa de ruta para establecer el código de origen BGP. Utilice la forma no para borrar una entrada.

set weight.- Utilice este comando de configuración del mapa de ruta para especificar el ancho BGP para la tabla de enrutamiento. Utilice la forma no de este comando para borrar una entrada.

show ip bgp.- Utilice este comando EXEC para visualizar las entradas de una tabla de enrutamiento BGP.

```
RouterA# show ip bgp
```

show ip bgp cidr-only.- Utilice este comando EXEC de privilegio para visualizar las rutas con máscaras de red no naturales (es decir, enrutamiento entre dominios sin clase, ClDR).

show ip bgp community.- Utilice este comando EXEC para visualizar rutas que pertenecen a comunidades específicas BGP.

show ip bgp community-list.- Utilice este comando EXEC para visual izar las rutas permitidas por la lista de la comunidad BGP.
show ip bgp dampened-paths.- Utilice este comando EXEC para visualizar las rutas dampened BGP.

show ip bgp filter-list.- Utilice este comando EXEC de privilegio para mostrar las rutas en función de una lista de filtro específica.

show ip bgp flap-statistics.- Utilice este comando EXEC para visualizar las estadísticas de las fluctuaciones BGP.

show ip bgp inconsistent-as.- Utilice este comando EXEC de privilegio para visualizar las rutas originadas por sistemas autónomos inconsistentes.

show ip bgp neighbors.- Utilice este comando EXEC para visualizar información acerca de las conexiones BGP y TCP con vecinos.

```
RouterA#sh ip bgp neighbors
```

show ip bgp paths.- Utilice este comando EXEC para visualizar todas las rutas BGP en la base de datos.

show ip bgp peer-group.- Utilice este comando EXEC para visualizar información sobre los grupos de iguales BGP.

show ip bgp regexp.- Utilice este comando EXEC de privilegio para visualizar las rutas que coinciden con la expresión regular.

```
RouterA#show ip bgp regexp ^100$
```

show ip bgp summary.- Utilice el comando EXEC para visualizar el estado de todas las conexiones BGP.

```
RouterA# show ip bgp summary
```

show ip prefix-list.- Utilice este comando EXEC para visualizar información sobre la lista de prefijos o acerca de las entradas de la misma.

synchronization.- Utilice este comando de configuración del router para habilitar la sincronización entre BGP y su sistema de Protocolo de gateway interior (IGP).

```
Router(config-router)#
synchronization
```

Utilice la forma no de este comando para permitir que el software Cisco IOS publique una ruta de red sin esperar al IGP.

```
Router(config-router)#
no synchronization
```

table-map.- Utilice este comando de configuración del router para modificar el métrico y los valores de las etiquetas cuando la tabla de enrutamiento IP se actualiza con las rutas aprendidas con BGP. Utilice la forma no de este comando para deshabilitar esta función.

timers bgp.- Utilice este comando de configuración del router para establecer los temporizadores de red BGP. Utilice la forma no de este comando para restablecer la temporización BGP predeterminada.

ANEXO 3

4.3 COMANDOS DE CONFIGURACIÓN IPv6 SOBRE EQUIPAMIENTO MARCA CISCO.

Configuración de direcciones estáticas de IPv6

```
R1(config)# interface serial0/0/0
R1(config-if)# ipv6 address FEC0::12:1/112
R1(config-if)# clockrate 64000
R1(config-if)# no shutdown
R1(config-if)# interface s0/0/1
R1(config-if)# ipv6 address FEC0::13:1/112
R1(config-if)# clockrate 64000
R1(config-if)# no shutdown

R2(config)# interface serial0/0/0
R2(config-if)# ipv6 address FEC0::12:2/112
R2(config-if)# no shutdown

R3(config)# interface serial0/0/0
R3(config-if)# ipv6 address FEC0::13:3/112
R3(config-if)# clockrate 64000
```

Muestra las interfaces del router

```
R1#show ipv6 interface serial 0/0/0
```

Muestra una breve interfaz de IPv6

```
R2#show ipv6 interface brief
```

Activación del enrutamiento IPv6 y CEF

La versión actual del IOS del enrutamiento IPv6 y CEF se encuentra deshabilitado por defecto. Para habilitar el enrutamiento de IPv6, use el comando de configuración global ipv6 unicast-routing.

```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 cef
```

Configuración del OSPFv3

A diferencia de IPv4 OSPF, donde las redes se suman al proceso de OSPF con declaraciones de la red bajo el protocolo de enrutamiento de configuración del sistema, IPv6 OSPF utiliza el símbolo del nivel de la interfaz IPv6 proceso de área OSPF área para agregar una interfaz a un área.

```
R1(config)#interface loopback0
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#interface serial0/0/0
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#interface serial0/0/1
R1(config-if)#ipv6 ospf 1 area 0
```

Comando para comprobar que los routers vecinos tienen OSPFv3.

```
R1#show ipv6 ospf neighbor
```

Comando para ver la tabla de enrutamiento

```
R1#show ipv6 route
```

Comando para mirar el comportamiento de la interfaz OSPF

```
R1#show ipv6 ospf interface
```

Configurar EIGRP

```
R1(config)# router eigrp 1
R1(config-router)# no auto-summary
R1(config-router)# network 10.0.0.0
R1(config-router)# network 172.16.0.0
```

Configuración manual del Túnel Ipv6

```
R1(config)# int tunnel0
R1(config-if)# tunnel mode ipv6ip
R1(config-if)# tunnel source s0/0/0
R1(config-if)# tunnel destination 172.16.23.3
R1(config-if)# ipv6 add FEC0::13:1/112
```

Configuración de Rutas estaticas IPv6

```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 route FEC0::3:0/112 2002:AC10:1703:1::3
```

Crear las interfaces Loopback.

Las interfaces loopback se utilizarán para muchas cosas. Esto incluye la generación de rutas (para ser publicadas) y la configuración de algunos peering para que sirve este comandos BGP. Cada equipo de enrutador particionará su bloque de direcciones y utilizará parte de éste para las interfaces Loopback.

```
Router1(config)#interface loopback 0
Router1(config-if)#ipv6 enable
Router1(config-if)#ipv6 address FEC0:200:4:7::1/128
```

Ping para IPv6

Sirve para verificar la conectividad de IP. Cuando esté resolviendo problemas, puede usar ping para enviar una solicitud de eco ICMP a un nombre de host de destino o a una dirección IP. Use ping siempre que necesite comprobar que un equipo host puede conectarse a la red TCP/IP y a los recursos de red. También puede usar ping para aislar problemas de hardware de red y configuraciones incompatibles.

```
R1#ping FEC0::12:2
```

Conexiones serie

```
R1(config)# interface serial0/0/0
R1(config-if)# ipv6 address FEC0::12:1/112
R1(config-if)# clockrate 64000
R1(config-if)# no shutdown
```

Configuración de Direcciones EUI-64

Las direcciones EUI-64 son direcciones donde los primeros 64 bits son la red de la parte de dirección y se especifica, y el segundo de 64 bits son la parte del host de la dirección y generado automaticamente por el dispositivo.

```
R2(config)# interface fastethernet0/0
R2(config-if)# ipv6 address FEC0:23::/64 eui-64
R2(config-if)# no shutdown
```

Cambiando la Dirección de enlace-local en una Interfaz

```
R1#show ipv6 interface serial 0/0/0
```

Activar routing para IPv6

```
Router1 (config)# ipv6 unicast-routing
```

Estableciendo OSPFv3

```
R1(config)#interface loopback0
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#interface serial0/0/0
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#interface serial0/0/1
R1(config-if)#ipv6 ospf 1 area 0
```

Comprobar OSPFv3 en función de IPv6

```
R1#show ipv6 ospf neighbor
```

Sumarización de áreas OSPFv3

```
R1#tclsh
```

Configuración de un Túnel Manual del IPv6

```
R1(config)# int tunnel0
R1(config-if)# tunnel mode ipv6ip
R1(config-if)# tunnel source s0/0/0
R1(config-if)# tunnel destination 172.16.23.3
R1(config-if)# ipv6 add FEC0::13:1/112
```

Configurar doble pila del IOS de Cisco

```
R1(config)# interface loopback0
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# ipv6 address FEC0::1:1/112
R1(config-if)# interface serial0/0/0
```

```
R1(config-if)# ip address 172.16.12.1 255.255.255.0
R1(config-if)# clockrate 64000
R1(config-if)# no shutdown
```

Configurar un servidor o servidores DNS para consultar

```
R1(config)#ip name-server address
R1(config)#ip name-server 3ffe:b00:ffff:b::1
```

- **Borrar rutas de la tabla de enrutamiento RIP IPv6**

```
clear ipv6 rip
```

- **Borrar todas las rutas de la tabla de enrutamiento IPv6**

```
clear ipv6 route *
```

- **Eliminar la ruta especifica de la tabla de enrutamiento IPv6**

clear ipv6 route 2001:db8:cl8:3::/64